

42125815.001.ІЕ.35

Система криптографічного захисту інформації «Шифр-Х.509»

Загальний опис

Зміст

СПИСОК СКОРОЧЕНЬ ТА УМОВНИХ ПОЗНАЧЕНЬ	4
ВВЕДЕННЯ	5
Загальний опис системи.....	5
СКЛАД ТА ОСНОВНІ ФУНКЦІЇ СКЗІ ШИФР-Х.509	7
Загальна характеристика	7
Підсистема сертифікації	12
Програмно-технічний комплекс «Центр сертифікації ключів».....	13
Відокремлений пункт реєстрації.....	16
Зберігання ключових даних, які потребують запису на носій.....	16
Зберігання особистих ключів чи інших ключових даних, які потребують захисту.....	17
Управління доступом до інформаційних ресурсів підсистеми сертифікації	17
Підсистеми криптографічного захисту даних	18
Бібліотека криптографічних функцій.....	18
Бібліотека функцій реєстрації.....	18
Підсистема організаційно-технічного захисту	19
ТЕХНОЛОГІЯ ФУНКЦІОНУВАННЯ ПІДСИСТЕМИ УПРАВЛІННЯ КЛЮЧАМИ ТА СЕРТИФІКАТАМИ	20
Загальні положення	20
Режими видачі сертифіката ЦСК	20
Профілі сертифікатів, які використовуються у підсистемі управління ключами	20
Режими генерації ключів адміністраторів підсистеми управління ключами.....	21
ТЕХНОЛОГІЯ ВСТАНОВЛЕННЯ ТА ІНІЦІАЛІЗАЦІЇ РОБОТИ ЦСК	22
Передумови встановлення та ініціалізації роботи ЦСК	22
Ключі та сертифікати системи внутрішньої автентифікації ЦСК.....	23
Технологія ініціалізації системи внутрішньої автентифікації та генерації ключів сертифікації ЦСК.....	23
Технологія завантаження кореневого сертифіката та сертифіката ЦСК.....	23
Технологія доступу та обміну даними між АРМ посадових осіб та сервером застосувань ЦСК	24
Технологія взаємодії засобами підсистеми сертифікації при розгортанні ЦР ЦСК.....	25
ТЕХНОЛОГІЯ ВСТАНОВЛЕННЯ ТА ІНІЦІАЛІЗАЦІЇ РОБОТИ ВПР.....	26
Передумови встановлення та ініціалізації роботи ВПР.....	26
Технологія взаємодії підсистеми сертифікації при розгортанні ВПР	26
ТЕХНОЛОГІЯ УПРАВЛІННЯ КЛЮЧАМИ ТА СЕРТИФІКАТАМИ КОРИСТУВАЧІВ	26
Загальна інформація	26
Генерація ключів користувачів безпосередньо у ЦР.....	26
ПЛАНОВА ЗМІНА КЛЮЧІВ ТА СЕРТИФІКАТІВ	28
Планова зміна ключів та сертифікатів співробітників ЦСК.....	28
Зміна ключів та сертифікатів користувача	28
ТЕХНОЛОГІЯ ФУНКЦІОНУВАННЯ ЗАСОБІВ ПІДСИСТЕМИ СЕРТИФІКАЦІЇ ПРИ СКАСУВАННІ, БЛОКУВАННІ ТА ВІДНОВЛЕННІ ДІЇ СЕРТИФІКАТІВ.....	28
Технологія формування, збереження та розсилка СВС	29
Технологія скасування, блокування та відновлення дії сертифікатів з адміністратором реєстрації (оператором ЦПД)	30
Технологія скасування та блокування дії сертифікатів на основі запитів користувачів.....	31
ТЕХНОЛОГІЯ ФУНКЦІОНУВАННЯ ПІДСИСТЕМИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ДАНИХ	32
ТЕХНОЛОГІЯ ФУНКЦІОНУВАННЯ БІБЛІОТЕК КРИПТОГРАФІЧНИХ ФУНКЦІЙ.....	32
Криптографічні перетворення	32
ТЕХНОЛОГІЯ КЛЮЧІВ УЗГОДЖЕННЯ СЕКРЕТУ ДЛЯ ЗАШИФРОВУВАННЯ ДАНИХ	33
Ключі узгодження секрету	33
Зашифрування даних.....	34
Розшифрування даних	34
Зміна ключів та сертифікатів	34

РОБОТА З ЕЛЕКТРОННИМИ ПОЗНАЧКАМИ ЧАСУ.....	34
Формування запиту на електронну позначку часу.....	34
Отримання відповіді на запит електронну позначки часу.....	35
Перевірка автентичності електронної позначки часу, яка зберігається разом з даними.....	35
ТЕХНОЛОГІЯ ФУНКЦІОНУВАННЯ БІБЛІОТЕК ФУНКЦІЙ РЕЄСТРАЦІЇ	35
ЗАГАЛЬНІ ТЕХНІЧНІ ХАРАКТЕРИСТИКИ	37
ХАРАКТЕРИСТИКА ВИДІВ ЗАБЕЗПЕЧЕННЯ	38
СИСТЕМНЕ ТА СПЕЦІАЛЬНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ	38
ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ.....	38
ДЖЕРЕЛА	39

Список скорочень та умовних позначень

HTTP	Hypertext Transfer Protocol
LDAP	Lightweight Directory Access Protocol
OCSF	Online Certificate Status Protocol
PIN	Personal Identification Number
PKCS#10	Certification Request Standard
PKCS#11	Cryptographic Token Interface
PKCS#7	Cryptographic Message Syntax Standard
TCP	Transmission Control Protocol
TSA	Time Stamping Authority
TSP	Time Stamping Protocol
APM	Автоматизоване робоче місце
БД	База даних
ВПР	Відокремлений пункт реєстрації
ДКЕ	Довготривалі ключові елементи
ЕП	Електронний підпис
ЗЦ	Засвідчувальний центр
КНЕДП	Кваліфікований надавач електронних довірчих послуг
МГК	Модуль генерації ключів
НСД	Несанкціонований доступ
ОС	Операційна система
ПЗ	Програмне забезпечення
ПТК	Програмно-технічний комплекс
СВС	Список відкликаних сертифікатів
СКЗІ	Система криптографічного захисту інформації
СУБД	Система управління базами даних
ЦЗО	Центральний засвідчувальний центр
ЦПД	Центр прийому дзвінків
ЦР	Центр реєстрації
ЦСК	Центр сертифікації ключів

Введення

Загальний опис системи

Система криптографічного захисту інформації «Шифр-Х.509» (СКЗІ «Шифр-Х.509») призначена для створення інфраструктури відкритих ключів, які входять у ЦСК, у тому числі Кваліфіковані надавачі електронних довірчих послуг (КНЕДП), ЦР у рамках відповідальності ЦСК, надає користувачам засоби управління ключами. Забезпечує послугами ЕП органи державної влади, органи місцевого самоврядування, підприємства, відомства та організації будь-якої форми власності, а також фізичних осіб.

Функціональне призначення СКЗІ «Шифр-Х.509» є:

- Забезпечення управління ключами та сертифікатами у відповідності з ДСТУ ISO/IEC 9594-8:2014 «Інформаційні технології. Взаємозв'язок відкритих систем. Каталог. Частина 8. Основні положення щодо сертифікації відкритих ключів та атрибутів»;
- Забезпечення криптографічного захисту конфіденційної та відкритої інформації: створення та перевірка електронного підпису, зашифрування та імітозахист даних.

СКЗІ «Шифр-Х.509» є програмним комплексом, засоби якого функціонують у середовищі ОС та взаємодіють із прикладним ПЗ.

Всі криптографічні перетворення у рамках СКЗІ «Шифр-Х.509» виконуються бібліотеками, які входять до складу програмного винаходу «Шифр+» v2.1, який має чинний позитивний експертний висновок, виданий Державною службою спеціального зв'язку та захисту інформації України від 16.05.2017, №04/03/02-1674.

СКЗІ «Шифр-Х.509» має чинний позитивний експертний висновок в області криптографічного захисту інформації, виданий Державною службою спеціального зв'язку та захисту інформації України від 05.05.2021, №04/05/02-1278.

Засоби підсистеми управління ключами та сертифікатами, які входять до складу СКЗІ «Шифр-Х.509», на алгоритмічному та програмному рівнях, є повноцінним виробом та призначений для використання у складі комплексу обробки та передачі інформації.

Засоби підсистеми криптографічного захисту даних СКЗІ «Шифр-Х.509» є окремими програмними компонентами (бібліотеками), які самостійно не експлуатуються та призначені для застосування, як складові частини при побудові комплексу обробки та передачі інформації.

Реалізація засобів СКЗІ «Шифр-Х.509» відповідають вимогам наступних нормативних документів:

- Закон України «Про електронні довірчі послуги» від 05.10.2017р. № 2155-VIII.
- Закон України «Про електронні документи та електронний документообіг» від 22.05.2003 г. № 851-IV.
- Постанова Кабінету Міністрів України від 10.05.2018 № 356 «Про внесення змін та визнання такими, що втратили чинність, деяких актів Кабінету Міністрів України у зв'язку з прийняттям Закону України «Про електронні довірчі послуги».
- Постанова Кабінету Міністрів України від 19.09.2018 № 749 «Про затвердження Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності».
- Постанова Кабінету Міністрів України від 07.11.2018 № 992 «Про затвердження вимог у сфері електронних довірчих послуг та Порядку перевірки дотримання вимог законодавства у сфері електронних довірчих послуг».
- Постанова Кабінету Міністрів України від 18.12.2018 № 1215 «Про затвердження Порядку проведення процедури оцінки відповідності у сфері електронних довірчих послуг».
- Постанова Кабінету Міністрів України від 03.03.2020 № 193 «Про реалізацію експериментального проекту щодо забезпечення можливості використання удосконалених електронних підписів і печаток, які базуються на кваліфікованих сертифікатах відкритих ключів».

- Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20.07.2007 № 141 «Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації». Зареєстровано в Міністерстві юстиції України 30 липня 2007 р. за № 862/14129.
- Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 18.12.2012 № 739 «Про затвердження Вимог до форматів криптографічних повідомлень». Зареєстровано в Міністерстві юстиції України 14 січня 2013 р. за № 108/22640.
- Про позначку кваліфікованого сертифіката відкритого ключа, затверджені Наказом Міністерства юстиції України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 01.02.2019 № 316/5/57. Зареєстровано в Міністерстві юстиції України 05 лютого 2019 р. за № 123/33094
- Наказ Міністерства юстиції України від 04.11.2019 № 3398/5 «Про затвердження Порядку подання до центрального засвідчувального органу інформації про діяльність надавачів електронних довірчих послуг та засвідчувального центру». Зареєстровано в Міністерстві юстиції України 07 листопада 2019 р. за № 1147/34118.
- Наказ Міністерства цифрової трансформації України від 28 липня 2020 року № 112 «Про затвердження Порядку ведення реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів», зареєстрований в Міністерстві юстиції України 18.08.2020 за № 798/35081.

Склад та основні функції СКЗІ Шифр-Х.509

Загальна характеристика

СКЗІ «Шифр-Х.509» складається з 3-х підсистем:

- Підсистеми сертифікації;
- Підсистеми криптографічного захисту даних;
- Підсистеми організаційно-технічного захисту.

СКЗІ «Шифр-Х.509» забезпечує:

- Управління ключами ЕП та шифрування, а також відповідними сертифікатами;
- Формування та перевірка ЕП;
- Управління ключами зашифрування даних;
- Зашифрування та розшифрування даних, їх імітозахист;
- Формування та перевірка електронної позначки часу.

Управління ключами та сертифікатами, формування електронних позначок часу виконуються у відповідності з вимогами стандартів та інших нормативних документів, які перераховані у Таблиця 1.

Таблиця 1. Перелік стандартів та рекомендацій реалізованих у СКЗІ

№	Стандарт	Назва стандарту
Стандарти, що визначають загальні вимоги до кваліфікованого надавача електронних довірчих послуг під час надання кваліфікованих електронних довірчих послуг		
1	ДСТУ ETSI TR 119 400:2017 (ETSI TR 119 400:2016, IDT)	Електронні підписи та інфраструктури (ESI). Настанова з використання стандартів провайдерів довірчих послуг, які підтримують цифрові підписи та пов'язані з ними послуги
2	ДСТУ ETSI EN 319 401:2016 (ETSI EN 319 401:2016, IDT)	Електронні підписи й інфраструктури (ESI). Загальні вимоги політики для провайдерів довірчих послуг
3	ДСТУ ETSI EN 319 403:2016 (ETSI EN 319 403:2015, IDT)	Електронні підписи та інфраструктури (ESI). Оцінювання відповідності провайдерів довірчих послуг. Вимоги до органів з оцінювання відповідності, що оцінюють провайдерів довірчих послуг
Стандарти, що визначають вимоги до Довірчого списку		
4	ДСТУ ETSI TR 119 600:2016 (ETSI TR 119 600:2016, IDT)	Електронні підписи та інфраструктури (ESI). Настанова щодо застосування стандартів для провайдерів переліків стану довірчих послуг
5	ДСТУ ETSI TS 119 612:2016 (ETSI TS 119 612:2016, IDT)	Електронні підписи та інфраструктури. Довірчі списки
Стандарти, що визначають вимоги до надання кваліфікованих електронних довірчих послуг, пов'язаних із створенням, перевіркою та підтвердженням електронних підписів, печаток, а також зберіганням кваліфікованих електронних підписів, печаток, електронних позначок часу та відповідних сертифікатів відкритих ключів		
6	ДСТУ ETSI TR 119 000:2017 (ETSI TR 119 000:2016, IDT)	Електронні підписи та інфраструктури (ESI). Модель стандартизації підписів. Огляд
7	ДСТУ ETSI TR 119 001:2017 (ETSI TR 119 001:2016, IDT)	Електронні підписи та інфраструктури (ESI). Модель стандартизації підписів. Визначення понять та скорочення
8	ДСТУ ETSI TR 119 100:2017 (ETSI TR 119 100:2016, IDT)	Електронні підписи та інфраструктури (ESI). Настанова з використання стандартів для створення та валідації підпису
9	ДСТУ ETSI TS 119 101:2016	Електронні підписи та інфраструктури. Вимоги та

	(ETSI TS 119 101:2016, IDT)	політики безпеки для додатків формування та перевірки підписів
10	ДСТУ ETSI EN 319 102-1:2016 (ETSI EN 319 102-1:2016, IDT)	Електронні підписи й інфраструктури (ESI). Процедури створення та перевірення цифрового підпису ADES. Частина 1. Створення та перевірення
11	ДСТУ ETSI EN 319 122-1:2016 (ETSI EN 319 122-1:2016, IDT)	Електронні підписи й інфраструктури (ESI). Цифрові підписи CAdES. Частина 1. Структурні блоки та базові підписи CAdES
12	ДСТУ ETSI EN 319 122-2:2016 (ETSI EN 319 122-2:2016, IDT)	Електронні підписи й інфраструктури (ESI). Цифрові підписи CAdES. Частина 2. Розширені підписи CAdES
13	ДСТУ ETSI EN 319 132-1:2016 (ETSI EN 319 132-1:2016, IDT)	Електронні підписи й інфраструктури (ESI). Цифрові підписи XAdES. Частина 1. Структурні блоки та базові підписи XAdES
14	ДСТУ ETSI EN 319 132-2:2016 (ETSI EN 319 132-2:2016, IDT)	Електронні підписи й інфраструктури (ESI). Цифрові підписи XAdES. Частина 2. Розширені підписи XAdES
15	ДСТУ ETSI EN 319 142-1:2016 (ETSI EN 319 142-1:2016, IDT)	Електронні підписи та інфраструктури. Цифрові підписи PAdES. Частина 1. Структурні елементи та базові PAdES підписи
16	ДСТУ ETSI EN 319 142-2:2016 (ETSI EN 319 142-2:2016, IDT)	Електронні підписи та інфраструктури. Цифрові підписи PAdES. Частина 2. Додаткові профілі підписів PAdES
17	ДСТУ ETSI EN 319 162-1:2016 (ETSI EN 319 162-1:2016, IDT)	Електронні підписи й інфраструктури (ESI). Контейнери, пов'язані з підписом (ASiC). Частина 1. Структурні блоки та базові контейнери ASiC
18	ДСТУ ETSI EN 319 162-2:2016 (ETSI EN 319 162-2:2016, IDT)	Електронні підписи й інфраструктури (ESI). Контейнери, пов'язані з підписом (ASiC). Частина 2. Додаткові контейнери ASiC
19	ДСТУ ETSI TS 102 778-1:2015 (ETSI TS 102 778-1:2009, IDT)	Електронні підписи та інфраструктура (ESI). Профілі розширених електронних підписів PDF. Частина 1. Огляд серії PAdES - базові принципи PAdES
20	ДСТУ ETSI TS 102 778-2:2015 (ETSI TS 102 778-2:2009, IDT)	Електронні підписи та інфраструктура (ESI). Профілі розширених електронних підписів PDF. Частина 2. Базовий PAdES - профілі, що базуються на ISO 32000-1
21	ДСТУ ETSI TS 102 778-3:2015 (ETSI TS 102 778-3:2010, IDT)	Електронні підписи та інфраструктура (ESI). Профілі розширених електронних підписів PDF. Частина 3. Посилений PAdES - профілі PAdES-BES і PAdES-EPES
22	ДСТУ ETSI TS 102 778-4:2015 (ETSI TS 102 778-4:2009, IDT)	Електронні підписи та інфраструктура (ESI). Профілі розширених електронних підписів PDF. Частина 4. Довгостроковий PAdES - профіль PAdES LTV
23	ДСТУ ETSI TS 102 778-5:2015 (ETSI TS 102 778-5:2009, IDT)	Електронні підписи та інфраструктура (ESI). Профілі розширених електронних підписів PDF. Частина 5. PAdES для XML контенту - профілі для підписів XAdES
Стандарти, що визначають вимоги до надання кваліфікованих електронних довірчих послуг, пов'язаних з формуванням, перевіркою та підтвердженням чинності кваліфікованих сертифікатів електронного підпису, печатки, автентифікації веб-сайту		
24	ДСТУ ETSI EN 319 411-1:2016 (ETSI EN 319 411-	Електронні підписи й інфраструктури (ESI). Вимоги політики та безпеки для провайдерів трастових

	1:2016, IDT)	послуг, які видають сертифікати. Частина 1. Загальні вимоги
25	ДСТУ ETSI EN 319 411-2:2016 (ETSI EN 319 411-2:2016, IDT)	Електронні підписи й інфраструктури (ESI). Вимоги політики та безпеки для провайдерів трастових послуг, які видають сертифікати. Частина 2. Вимоги до провайдерів трастових послуг, які видають кваліфіковані сертифікати ЄС
Стандарти, що визначають вимоги до надання кваліфікованої електронної довірчої послуги з формування, перевірки та підтвердження кваліфікованої електронної позначки часу		
26	ДСТУ ETSI EN 319 421:2016 (ETSI EN 319 421:2016, IDT)	Електронні підписи й інфраструктури (ESI). Політика та вимоги безпеки щодо провайдерів трастових послуг, які видають часові штампелі
27	ДСТУ ETSI EN 319 422:2016 (ETSI EN 319 422:2016, IDT)	Електронні підписи та інфраструктури. Протокол мітки часу та профілі токенів мітки часу
Стандарти, що визначають вимоги до засобів кваліфікованого електронного підпису чи печатки		
28	ДСТУ EN 419211-1:2016 (EN 419211-1:2014, IDT)	Профілі захисту для пристроїв створення безпечного підпису. Частина 1. Огляд
29	ДСТУ EN 419211-2:2016 (EN 419211-2:2013, IDT)	Профілі захисту для пристроїв створення безпечного підпису. Частина 2. Пристрій з генерацією ключів
30	ДСТУ EN 419211-3:2016 (EN 419211-3:2013, IDT)	Профілі захисту для пристроїв створення безпечного підпису. Частина 3. Пристрій з імпортом ключів
31	ДСТУ EN 419211-4:2016 (EN 419211-4:2013, IDT)	Профілі захисту для пристроїв створення безпечного підпису. Частина 4. Розширення для пристроїв з генерацією ключів та довіреним каналом для застосування генерації сертифікатів
32	ДСТУ EN 419211-5:2016 (EN 419211-5:2013, IDT)	Профілі захисту для пристроїв створення безпечного підпису. Частина 5. Розширення для пристроїв з генерацією ключів та довіреним каналом для застосування створення підпису
33	ДСТУ EN 419211-6:2016 (EN 419211-6:2014, IDT)	Профілі захисту для пристроїв створення безпечного підпису. Частина 6. Розширення для пристроїв з імпортом ключів та довіреним каналом для застосування створення підпису
34	ДСТУ ISO/IEC 19790:2015 (ISO/IEC 19790:2012, IDT)	Інформаційні технології. Методи захисту. Вимоги безпеки до криптографічних модулів
Стандарти, що визначають вимоги до кваліфікованих сертифікатів відкритих ключів		
35	ДСТУ ISO/IEC 9594-8:2014 (ISO/IEC 9594-8:2014, IDT)	Інформаційні технології. Взаємозв'язок відкритих систем. Каталог. Частина 8. Основні положення щодо сертифікації відкритих ключів та атрибутів
36	ДСТУ ETSI EN 319 412-1:2016 (ETSI EN 319 412-1:2016, IDT)	Електронні підписи й інфраструктури (ESI). Профілі сертифікатів. Частина 1. Огляд та типові структури даних
37	ДСТУ ETSI EN 319 412-2:2016 (ETSI EN 319 412-2:2016, IDT)	Електронні підписи та інфраструктури. Профілі сертифікатів. Частина 2. Профілі сертифікатів, випущених для фізичних осіб
38	ДСТУ ETSI EN 319 412-3:2016 (ETSI EN 319 412-3:2016, IDT)	Електронні підписи та інфраструктури (ESI). Профілі сертифікатів. Частина 3. Профіль сертифіката юридичної особи

39	ДСТУ ETSI EN 319 412-4:2016 (ETSI EN 319 412-4:2016, IDT)	Електронні підписи й інфраструктури (ESI). Профілі сертифікатів. Частина 4. Профіль сертифіката для сертифікатів веб-сайтів
40	ДСТУ ETSI EN 319 412-5:2016 (ETSI EN 319 412-5:2016, IDT)	Електронні підписи та інфраструктури. Профілі сертифікатів. Частина 5. Системи контролю якості
Стандарти, що визначають вимоги до надання кваліфікованої електронної довірчої послуги з реєстрованої електронної доставки		
41	ДСТУ ETSI EN 319 522-1:2018 (ETSI EN 319 522-1:2018, IDT)	Електронні підписи та інфраструктури (ESI). Служби реєстрованого електронного доставляння. Частина 1. Модель та архітектура
42	ДСТУ ETSI EN 319 522-2:2018 (ETSI EN 319 522-2:2018, IDT)	Електронні підписи та інфраструктури (ESI). Служби реєстрованого електронного доставляння. Частина 2. Семантика вмісту
43	ДСТУ ETSI EN 319 522-3:2018 (ETSI EN 319 522-3:2018, IDT)	Електронні підписи та інфраструктури (ESI). Служби реєстрованого електронного доставляння. Частина 3. Формати
44	ДСТУ ETSI EN 319 522-4-1:2018 (ETSI EN 319 522-4-1:2018, IDT)	Електронні підписи та інфраструктури (ESI). Служби реєстрованого електронного доставляння. Частина 4. Прив'язки. Секція 1. Прив'язки доставляння повідомлень
45	ДСТУ ETSI EN 319 522-4-2:2018 (ETSI EN 319 522-4-2:2018, IDT)	Електронні підписи та інфраструктури (ESI). Служби реєстрованого електронного доставляння. Частина 4. Прив'язки. Секція 2. Прив'язки доказів та ідентифікації
46	ДСТУ ETSI EN 319 522-4-3:2018 (ETSI EN 319 522-4-3:2018, IDT)	Електронні підписи та інфраструктури (ESI). Служби реєстрованого електронного доставляння. Частина 4. Прив'язки. Секція 3. Прив'язка можливостей/вимог
47	ДСТУ ETSI EN 319 532-1:2018 (ETSI EN 319 532-1:2018, IDT)	Електронні підписи та інфраструктури (ESI). Служби реєстрованої електронної пошти (REM). Частина 1. Модель та архітектура
48	ДСТУ ETSI EN 319 532-2:2018 (ETSI EN 319 532-2:2018, IDT)	Електронні підписи та інфраструктури (ESI). Служби реєстрованої електронної пошти (REM). Частина 2. Семантика вмісту
49	ДСТУ ETSI EN 319 532-3:2018 (ETSI EN 319 532-3:2018, IDT)	Електронні підписи та інфраструктури (ESI). Служби реєстрованої електронної пошти (REM). Частина 3. Формати
50	ДСТУ ETSI EN 319 532-4:2018 (ETSI EN 319 532-4:2018, IDT)	Електронні підписи та інфраструктури (ESI). Служби реєстрованої електронної пошти (REM). Частина 4. Профілі інтероперабельності
Стандарти, що визначають вимоги до криптографічного захисту інформації		
51	ДСТУ 4145:2002	Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння
52	ДСТУ 7564:2014	Інформаційні технології. Криптографічний захист інформації. Функція гешування
53	ДСТУ 7624:2014	Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення

54	ДСТУ ETSI TR 119 300:2016 (ETSI TR 119 300:2016, IDT)	Електронні підписи та інфраструктури (ESI). Настанова щодо застосування стандартів для криптографічних комплектів
55	ДСТУ ETSI TS 119 312:2015 (ETSI TS 119 312:2014, IDT)	Електронні підписи й інфраструктури (ESI). Криптографічні комплекти
56	ДСТУ ISO/IEC 14888-1:2015 (ISO/IEC 14888-1:2008, IDT)	Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 1. Загальні положення
57	ДСТУ ISO/IEC 14888-2:2015 (ISO/IEC 14888-2:2008, IDT)	Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 2. Механізми, що ґрунтуються на факторизації цілих чисел
58	ДСТУ ISO/IEC 14888-3:2015 (ISO/IEC 4888-3:2006; Cor 1:2007; Cor 2:2009; Amd 1:2010; Amd 2:2012, IDT)	Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 3. Механізми, що ґрунтуються на дискретному логарифмуванні
Стандарти, що визначають вимоги до інформаційної безпеки		
59	ДСТУ ISO/IEC 18045:2015 (ISO/IEC 18045:2008, IDT)	Інформаційні технології. Методи захисту. Методологія оцінювання безпеки ІТ
60	ДСТУ ISO/IEC 15408-1:2017 (ISO/IEC 15408-1:2009, IDT)	Інформаційні технології. Методи захисту. Критерії оцінки. Частина 1. Вступ та загальна модель
61	ДСТУ ISO/IEC 15408-2:2017 (ISO/IEC 15408-2:2008, IDT)	Інформаційні технології. Методи захисту. Критерії оцінки. Частина 2. Функціональні вимоги
62	ДСТУ ISO/IEC 15408-3:2017 (ISO/IEC 15408-3:2008, IDT)	Інформаційні технології. Методи захисту. Критерії оцінки. Частина 3. Вимоги до гарантії безпеки
63	ДСТУ ISO/IEC 27001:2015 (ISO/IEC 27001:2013; Cor 1:2014, IDT)	Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги
64	ДСТУ ISO/IEC 27002:2015 (ISO/IEC 27002:2013; Cor 1:2014, IDT)	Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки
65	ДСТУ ISO/IEC 27005:2015 (ISO/IEC 27005:2011, IDT)	Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки
Стандарти щодо тестування інтероперабельності		
66	ДСТУ ETSI SR 003 186:2017 (ETSI SR 003 186:2016, IDT)	Електронні підписи та інфраструктури (ESI). Тестування інтероперабельності та заходи, необхідні для імплементації та популяризації моделі цифрових підписів
67	ДСТУ ETSI TS 119 124-4:2017 (ETSI TS 119 124-4:2016, IDT)	Електронні підписи та інфраструктури (ESI). Цифрові підписи CAdES. Перевірка на відповідність і інтероперабельність. Частина 4. Тестування на відповідність базових підписів CAdES
68	ДСТУ ETSI TR 119 134-1:2017 (ETSI TR 119 134-1:2016, IDT)	Електронні підписи та інфраструктури (ESI). Цифрові підписи XAdES. Тестування на відповідність та інтероперабельність. Частина 1. Огляд
69	ДСТУ ETSI TR 119 134-2:2017 (ETSI TR 119 134-2:2016, IDT)	Електронні підписи та інфраструктури (ESI). Цифрові підписи XAdES. Тестування на відповідність та інтероперабельність. Частина 2. Набори тестів для тестування інтероперабельності базових підписів XAdES
70	ДСТУ ETSI TR 119 134-3:2017	Електронні підписи та інфраструктури (ESI).

	(ETSI TR 119 134-3:2016, IDT)	Цифрові підписи XAdES. Тестування на відповідність та інтероперабельність. Частина 3. Набори тестів для тестування інтероперабельності посилених підписів XAdES
71	ДСТУ ETSI TR 119 134-4:2017 (ETSI TR 119 134-4:2016, IDT)	Електронні підписи та інфраструктури (ESI). Цифрові підписи XAdES. Тестування на відповідність та інтероперабельність. Частина 4. Тестування на відповідність базовим підписам XAdES
72	ДСТУ ETSI TR 119 134-5:2017 (ETSI TR 119 134-5:2016, IDT)	Електронні підписи та інфраструктури (ESI). Цифрові підписи XAdES. Тестування на відповідність та інтероперабельність. Частина 5. Тестування на відповідність посилених підписів XAdES
73	ДСТУ ETSI TR 119 144-1:2017 (ETSI TR 119 144-1:2016, IDT)	Електронні підписи та інфраструктури (ESI). Цифрові підписи PAdES. Тестування відповідності та інтероперабельності. Частина 1. Огляд
74	ДСТУ ETSI TS 119 144-2:2017 (ETSI TS 119 144-2:2016, IDT)	Електронні підписи та інфраструктури (ESI). Цифрові підписи PAdES. Тестування відповідності та інтероперабельності. Частина 2. Набори тестів для тестування інтероперабельності базових підписів PAdES
75	ДСТУ ETSI TS 119 144-3:2017 (ETSI TS 119 144-3:2016, IDT)	Електронні підписи та інфраструктури (ESI). Цифрові підписи PAdES. Тестування відповідності та інтероперабельності. Частина 3. Набори тестів для тестування інтероперабельності додаткових підписів PAdES
76	ДСТУ ETSI TS 119 144-4:2017 (ETSI TS 119 144-4:2016, IDT)	Електронні підписи та інфраструктури (ESI). Цифрові підписи PAdES. Тестування відповідності та інтероперабельності. Частина 4. Тестування відповідності базових підписів PAdES
77	ДСТУ ETSI TS 119 144-5:2017 (ETSI TS 119 144-5:2016, IDT)	Електронні підписи та інфраструктури (ESI). Цифрові підписи PAdES. Тестування відповідності та інтероперабельності. Частина 5. Тестування відповідності додаткових підписів PAdES

Підсистема сертифікації

Підсистема сертифікації СКЗІ «Шифр-Х.509» може бути реалізована:

- Централізовано.
- Децентралізовано.

На Рис. 1 зображена структурна схема ЦСК із централізованим єдиним ЦР та віддаленими робочими місцями для роботи.

На Рис. 2 зображена структурна схема ЦСК із центральним ЦР, який знаходиться при ЦСК, а також ВПР, які знаходяться в окремих підрозділах чи організаціях.

Підсистема сертифікації, складається з наступних засобів:

- ПТК ЦСК у складі:
 - ПЗ сертифікації ключів;
 - ПЗ центру реєстрації;
 - LDAP-сервер;
 - OCSP-сервер;
 - TSP-сервер;
 - CMP-сервер;
 - Програмне забезпечення АРМ оператора ЦПД;
- Програмне забезпечення ВПР – програмне забезпечення центра реєстрації;
- Програмне забезпечення користувачів:
 - Win-32 бібліотека (модуль криптофункцій);

- Java-застосування для управління ключами та захисту даних;
- Microsoft Outlook 2010, 2013 Crypto Add-in;
- Microsoft Word 2010, 2013 Crypto Add-in;
- Microsoft Excel 2010, 2013 Crypto Add-in.
- Microsoft PowerPoint 2010, 2013 Crypto Add-in.

Програмно-технічний комплекс «Центр сертифікації ключів»

ПТК ЦСК призначений для реалізації регламентних процедур та механізмів роботи ЦСК, пов'язаних з обслуговуванням сертифікатів відкритих ключів, які включають:

- Управління ключами ЦСК;
- Реєстрація користувачів;
- Сертифікація відкритих ключів користувачів;
- Розповсюдження сертифікатів;
- Управління статусів сертифікатів;
- Розповсюдження інформації про статус сертифікатів;
- Надання послуг електронних позначок часу.

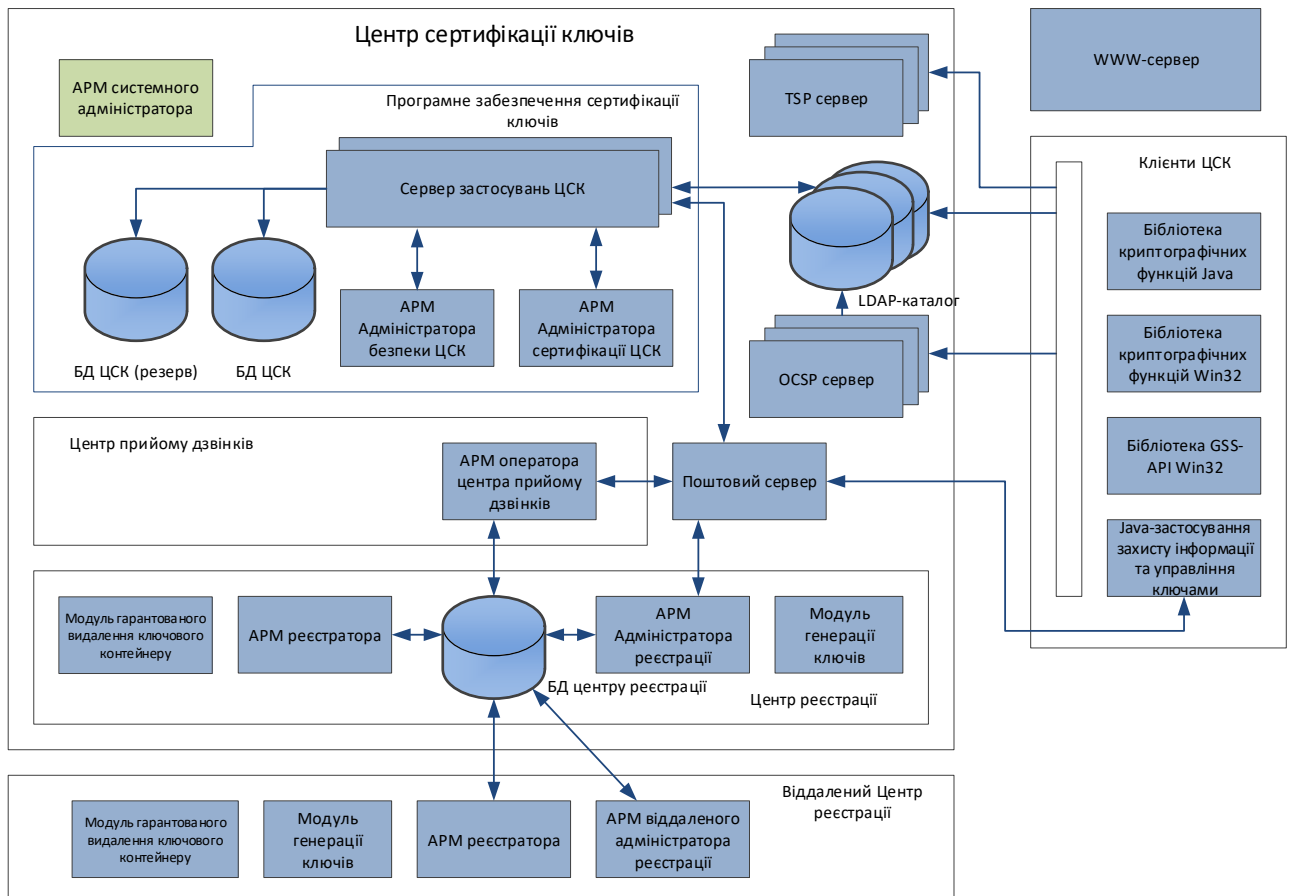


Рис. 1. Підсистеми управління ключами та сертифікатами

Програмні засоби сертифікації ключів

Склад ПЗ сертифікації ключів наступний:

- АРМ адміністратора безпеки та аудиту;
- АРМ адміністратора сертифікації;
- Сервер застосувань ЦСК;
- БД ЦСК;
- Загальний довідник на базі LDAP-каталогу.

Основними функціями програмних засобів сертифікації ключів є:

- створення, перевірка та підтвердження вдосконаленого електронного підпису чи печатки;
- формування, перевірка та підтвердження чинності сертифіката електронного підпису чи печатки;

- формування, перевірка та підтвердження чинності сертифіката автентифікації веб-сайту;
- формування, перевірка та підтвердження електронної позначки часу;
- зберігання вдосконалених електронних підписів, печаток, електронних позначок часу та сертифікатів, пов'язаних з цими послугами (реалізовано у іншому рішенні від компанії Сайфер – «Шифр-Arch»).

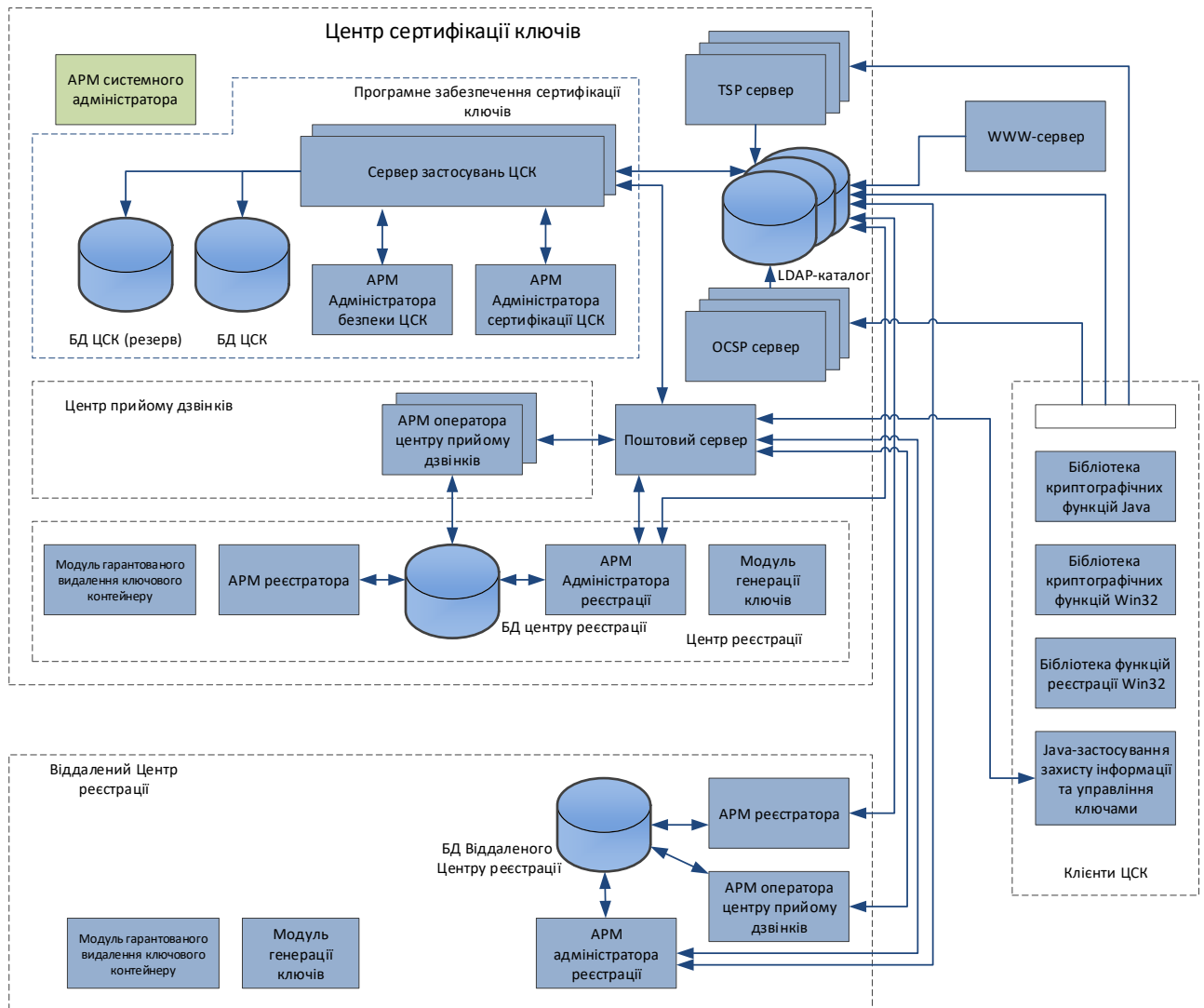


Рис. 2. Підсистема управління ключами та сертифікатами

Програмні засоби ЦР

Програмні засоби ЦР призначені для ідентифікації та реєстрації користувачів, які звертаються для отримання сертифікатів, а також для надання послуг генерації ключів користувачам, які мають бажання здійснити цю операцію безпосередньо у ЦР.

Засоби ЦР складаються з наступних ПЗ:

- АРМ адміністратора реєстрації;
- АРМ реєстратора;
- БД ЦР;
- Комунікаційний модуль;
- Локальний довідник сертифікатів на базі LDAP-сервера (необов'язковий елемент, може бути розгорнутий за необхідності на віддалених ЦР);
- АРМ оператора ЦРД (необов'язковий елемент, може бути розгорнутий за необхідності на віддалених ЦР);
- АРМ віддаленого адміністратора реєстрації (необов'язковий елемент, може бути розгорнутий за необхідності, як у центральному ЦР, так і на віддалених ЦР, у випадку централізованої, так і децентралізованої моделі побудови ЦР);
- Модуль генерації ключів;

- Модуль гарантованого знищення ключового контейнера.

Основними функціями ЦР є:

- Розмежування доступу до функцій та даних ЦР;
- Управління ключами адміністратора реєстрації;
- Управління ключами оператора реєстрації;
- Управління ключами оператора ЦПД;
- Управління ключами віддаленого адміністратора реєстрації;
- Ідентифікація та реєстрація користувачів;
- Видача стартових сертифікатів користувачам;
- Генерація робочих ключів для користувачів, які мають бажання отримати робочі сертифікати безпосередньо на ЦР, формування відповідних запитів на сертифікати;
- Гарантоване знищення ключового контейнера НКІ.
- Прийом та перевірка автентичності запитів на сертифікати користувачів;
- Прийом та перевірка автентичності запитів на скасування/блокування/відновлення сертифікатів користувачів;
- Підтвердження запитів на сертифікати користувачів підписуючи оператором реєстрації;
- Підтвердження запитів на сертифікати користувачів підписуючи адміністратором реєстрації;
- Підтвердження запитів на скасування/блокування/відновлення сертифікатів користувачів підписуючи адміністратором реєстрації;
- Підтвердження запитів на сертифікати користувачів підписуючи віддаленим адміністратором реєстрації;
- Підтвердження запитів на скасування/блокування/відновлення сертифікатів користувачів підписуючи віддаленим адміністратором реєстрації;
- Підтвердження запитів на скасування/блокування/відновлення сертифікатів користувачів підписуючи оператором ЦПД;
- Передача запитів на сертифікати до ЦСК електронною поштою чи експортуючи до заданого каталогу у вигляді файлу чи на носій;
- Передача запитів на скасування/блокування/відновлення сертифікатів ЦСК електронною поштою чи експортуючи до заданого каталогу у вигляді файлу чи на носій;
- Прийом та контроль автентичності сертифікатів користувачів з CBC;
- Видача сертифікатів користувачам, які мають бажання здійснити цю операцію безпосередньо на ЦР чи віддаленому ЦР.
- Передача сертифікатів та CBC на адресу користувачів, які генерують свої ключі самостійно;
- Ведення та аудит локальної БД сертифікатів ЦР чи віддаленого ЦР, а також запитів на сертифікат чи запитів на відкликання сертифікатів;
- Управління локальним довідником сертифікатів: розміщення, видалення сертифікатів у LDAP-каталозі.

LDAP-сервер

Програмне забезпечення сервера LDAP функціонує у відповідності з вимогами RFC 4511 «Lightweight Directory Access Protocol – LDAP» та призначений для зберігання та надання доступу користувачам до опублікованих сертифікатів та CBC за протоколом TCP/IP.

LDAP-сервер (каталог) призначений для створення довідника сертифікатів ЦСК. LDAP-сервер забезпечує зберігання та надання доступу користувача до опублікованих сертифікатів та CBC, які видаються ЦСК.

Сервер OCSP

Програмне забезпечення сервера OCSP функціонує у відповідності з вимогами RFC 6960 «Online Certificate Status Protocol – OCSP» та призначений для передачі користувачам інформації про статус сертифіката в інтерактивному режимі за протоколом TCP/IP або HTTP.

Сервер TSP

Програмне забезпечення сервера TSP функціонує у відповідності з вимогами RFC 5816 «Time-Stamp Protocol - TSP» та призначений для формування та передачі позначок часу для користувачів в інтерактивному режимі за протоколом TCP/IP або HTTP.

Сервер CMP

Програмне забезпечення сервера CMP функціонує у відповідності з вимогами RFC 6712 «Certificate Management Protocol - CMP» та призначений для передачі сертифікатів та CBC в інтерактивному режимі за протоколом TCP/IP або HTTP.

Програмне забезпечення АРМ оператора ЦПД

Програмне забезпечення АРМ оператора ЦПД призначене для виконання дій, пов'язаних з управлінням статусу сертифікатів на вимогу користувачів, котрим ці сертифікати належать.

Основними функціями ПЗ АРМ Оператора ЦПД є:

- Пошук та відбір сертифікатів для зміни їх статусу у відповідності заяв користувачів;
- Формування запитів на скасування, блокування, відновлення дій сертифікатів;
- Підтвердження запитів на скасування, блокування, відновлення дій сертифікатів, з підписом оператора ЦПД та їх передача до ЦСК.

Відокремлений пункт реєстрації

Для спрощення надання послуг з видачі сертифікатів користувачам, які територіально віддалені від ЦСК, розгортаються ВПР.

Як було вказано раніше, підтримуються кілька моделей ВПР:

- Централізована.
- Децентралізована.

У централізованій моделі, у відокремленому ПР розміщуються віддалені робочі місця єдиного ЦР, в той час, як у децентралізованій моделі відокремлених ПР розміщується повноцінний ЦР, з власною локальною БД ЦР та власним локальним LDAP-каталогом.

Підхід з децентралізованою моделлю реалізується для побудови ВПР в окремих організаціях та територіально розподілених підрозділах, які активно працюють з LDAP-каталогом. При цьому, здійснюється розмежування доступу до сертифікатів у LDAP-каталозі.

ВПР за складом ПЗ, а також виконувані функції ідентичні ПЗ ЦР, які функціонують у складі ЦСК.

Зберігання ключових даних, які потребують запису на носій

Незалежно від типу НКІ, у контейнері зберігаються наступні дані:

- Особисті ключі (чергові, діючі, для різних алгоритмів та призначення (ЕП та шифрування));
- Сертифікати (власника ключового контейнеру та ЦСК);
- Запити на сертифікат (до моменту, поки не отримано відповідного сертифікату).

Під НКІ мається на увазі:

- Файловий контейнер (чи ключовий контейнер), дані зберігаються у форматі PKCS#12, при цьому кількість ключів та сертифікатів для запису у контейнер може обмежуватися лише файловою системою.
- Захищений носій у пасивному режимі за протоколом PKCS#11, дані зберігаються у форматі PKCS#12 в контейнері даних носія, при цьому кількість ключів та сертифікатів для запису у контейнер може обмежуватися об'ємом пам'яті носія.
- Захищений носій у активному режимі за протоколом PKCS#11, ключі та сертифікати зберігаються в призначеному на носії місці, інші дані зберігаються у форматі PKCS#12 в контейнері даних носія, кількість та тип ключів, кількість сертифікатів, які можуть бути записані у контейнер можуть обмежуватися об'ємом пам'яті носія.

- Мережний криптографічний модуль, ключі та сертифікати зберігаються в призначеному на модулі місці, інші дані зберігаються у форматі PKCS#12 в контейнері даних модуля, кількість та тип ключів, кількість сертифікатів, які можуть бути записані у контейнер можуть обмежуватися виробником модулю.

Чинні відкриті ключі ЕП зберігаються безпосередньо, як ключі чи як сертифікати. Чинні відкриті ключі за протоколом Діффі-Хелмана, які використовуються при управлінні зашифрованих даних.

Чергові відкриті ключі ЕП зберігаються безпосередньо, як ключі, так і у вигляді відповідних запитів на сертифікат.

Зберігання особистих ключів чи інших ключових даних, які потребують захисту

Підсистема сертифікації забезпечує підвищений рівень безпеки відповідно зберігання наступних ключових даних:

- Особисті ключі (чергові, діючі, для різних алгоритмів та призначення (ЕП та шифрування));
- Сертифікати (власника ключового контейнеру та ЦСК);
- Запити на сертифікат (до моменту, поки не отримано відповідного сертифікату).

Перераховані ключові дані зберігаються:

- У складі ключового контейнера виключно у зашифрованому вигляді. Зашифровування виконується у відповідності з вимогами до блочного симетричного шифру у режимі гамування.
- Захищений носій у пасивному режимі, який підтримує PKCS#11 інтерфейс взаємодії.
- Захищений носій у активному режимі, який підтримує PKCS#11 інтерфейс взаємодії.
- Мережний криптографічний модуль, який підтримує PKCS#11 інтерфейс взаємодії.

Опис процесу зберігання особистого ключа ЦСК, наведена в документі – методика зберігання особистого ключа ЦСК [2].

Захист даних особистого ключа посадової особи ЦСК (адміністратора безпеки та аудиту ЦСК, адміністратора сертифікації ЦСК, адміністратора реєстрації ЦСК):

- У файловому НКІ, відповідно до PKCS#12.
- У захищеному НКІ, засобами самого носія. Крім того, носій зберігає сертифікат відкритого ключа та відповідну інформацію про ідентифікатор особистого ключа.
- У МКМ, засобами самого модулю.

Управління доступом до інформаційних ресурсів підсистеми сертифікації

Засоби підсистеми сертифікації забезпечують:

- Адміністрування з метою розмежування доступу обслуговуючого персоналу до ресурсів підсистеми, надання функцій тільки у відповідності з ролями обслуговуючого персоналу.
- Ідентифікація та автентифікація обслуговуючого персоналу перед початком виконання процедур, пов'язаних із формуванням сертифікату чи зміною його статусу.
- Протоколювання всіх дій обслуговуючого персоналу, пов'язаних з генерацією ключів, формуванням сертифікату чи зміною його статусу із забезпечення захисту протоколів від несанкціонованого доступу.

Журнали аудиту мають захист від НСД та модифікації. Засоби підсистеми забезпечують реєстрацію таких подій:

- Генерація ключів.
- Формування, переформування, блокування, скасування чи відновлення ключів, а також формування СВС.
- Спроби НСД.
- Надання доступу до засобів підсистеми.
- Збої у роботі засобів підсистеми.

Всі записи у журналі аудиту захищені імітовставкою, містять дату та час подій, а також ідентифікують суб'єкта, який ініціював дану подію.

Підсистеми криптографічного захисту даних

Підсистема криптографічного захисту даних складається із наступних програмних засобів:

- Бібліотека криптографічних функцій для підсистеми Win32;
- Бібліотека функцій для роботи з пристроями за інтерфейсом PKCS#11 для підсистеми Win32;
- Бібліотека криптографічних функцій для Java;
- Бібліотека функцій для роботи з пристроями за інтерфейсом PKCS#11 Java;
- Бібліотека функцій реєстрації для підсистеми Win32.

Бібліотека криптографічних функцій

Бібліотека криптографічних функцій для підсистеми Win32, а також у вигляді Java-класів забезпечують виконання наступних функцій:

- Генерація ключів ЕП, симетричного шифрування та узгодження секрету.
- Введення, розшифрування та збереження у пам'яті особистих ключів.
- Пошук та вибір сертифікату чи запиту із БД та отримання сертифікату із LDAP-каталогу.
- Пошук сертифікатів за ідентифікатором ключа з СМР-серверу.
- Контроль автентичності сертифіката.
- Контроль статусу сертифіката за CBC, чи запитом до OCSP-серверу.
- Блокування роботи програми, якщо строк дії сертифікату закінчено чи сертифікат скасовано або заблоковано.
- Створення та перевірка ЕП.
- Узгодження ключа зашифрованих даних.
- Зашифрування та розшифрування даних.
- Обчислення гешу даних.
- Зміна ключів користувача.
- Зміна пароллю доступу до НКІ.
- Формування запиту на електронну позначку часу, його передача на сервер TSP;
- Прийом відповіді від сервера TSP та перевірка автентичності електронної позначки часу.
- Знищення у пам'яті особистих ключів при деініціалізації роботи.

Криптографічні операції відбуваються на НКІ, а саме:

- У пам'яті комп'ютера.
- У файловому НКІ.
- У захищеному НКІ.
- У МКМ.

Бібліотека функцій реєстрації

Бібліотека функцій реєстрації у вигляді Win32 бібліотеки, призначена для виконання процедури генерації ключів, реєстрації запитів на сертифікат, запитів на скасування, блокування та відновлення сертифікату

Забезпечує виконання наступних функцій:

- Генерація ключів користувача з наступним формуванням запитів на сертифікат у форматі PKCS#10.
- Засвідчення запитів на сертифікат у форматі PKCS#7.
- Засвідчення запитів на сертифікат з формуванням стартових сертифікатів, засвідчених відповідною посадовою особою ЦСК.
- Збереження сформованих запитів та стартових сертифікатів у БД ЦР.
- Формування запитів на блокування, відновлення та скасування сертифікатів.
- Контроль статусу сформованих запитів на сертифікат та запитів на блокування, відновлення та скасування сертифікатів.
- Контроль статусів сертифікатів на основі CBC, які зберігаються у БД ЦР.
- Пошук та отримання X.509-об'єктів із ключових контейнерів особистих ключів.
- Збереження та видалення сертифікатів у НКІ.
- Отримання текстового представлення X.509-об'єктів у форматі HTML.
- Пошук дескрипторів X.509-об'єктів у БД ЦР.

- Видалення Х.509-об'єктів, сформованих поточним адміністратором та оператором реєстрації, з БД ЦР.
- Управління НКІ адміністраторів та користувачів:
 - Зміна ключів з наступним формуванням запиту на сертифікат;
 - Збереження запиту на сертифікат у БД ЦР;
 - Реєстрація сформованого сертифіката та введення в дію ключів.

Операції управління НКІ адміністраторів відбуваються:

- У пам'яті комп'ютера.
- У файловому НКІ.
- У захищеному НКІ.
- У МКМ.

Підсистема організаційно-технічного захисту

Підсистема організаційно-технічного захисту складається з наступних інструкцій посадовим особам та користувачам [4]:

- Інструкція із забезпечення безпеки експлуатації КНЕДП.
- Інструкція про порядок генерації ключових даних та поводження (обліку, зберігання, знищення) з ключовими документами [3].

У вищевказаних інструкціях відображається наступне:

- Права та обов'язки осіб, відповідальних за забезпечення безпеки експлуатації засобів СКЗІ «Шифр-Х.509»;
- Права та обов'язки користувачів послуг СКЗІ «Шифр-Х.509»;
- Порядок забезпечення безпеки засобів СКЗІ «Шифр-Х.509» під час їх встановлення, експлуатації, виведення їх з експлуатації, ремонту, а також у випадку порушення функціонування інформаційно-телекомунікаційної системи;
- Питання проведення тестування засобів СКЗІ «Шифр-Х.509» та їх резервування;
- Дії персоналу в умовах надзвичайних ситуаціях, стихійних лих чи підозра на компрометацію ключа;
- Порядок проведення контролю за станом забезпечення безпеки засобами СКЗІ «Шифр-Х.509»;
- Порядок допуску у приміщення, в яких встановлені засоби СКЗІ «Шифр-Х.509».

Технологія функціонування підсистеми управління ключами та сертифікатами

Загальні положення

Режими видачі сертифіката ЦСК

Поточна версія засобів «Шифр-Х.509» підтримує два режими видачі сертифікатів ЦСК:

- Самовидання кореневого сертифіката ЦСК.
- Видача сертифіката у вищестоящому ЦСК чи ЗЦ/ЦЗО.

Режим самовидання призначений для експлуатації комплексу в рамках корпоративної мережі окремого підприємства. В даному режимі сертифікат ЦСК формується безпосередньо у процесі генерації ключів шляхом самовидачі.

Режим виготовлення у вищестоящому ЦСК чи ЗЦ/ЦЗО, на основі запиту на сертифікат, може бути використаний для експлуатації комплексу в рамках міжкорпоративної мережі різних організацій. У процесі генерації ключів генерується запит на сертифікат ЦСК, який повинен бути переданий для реєстрації у ЗЦ/ЦЗО більш високого рівня. Після формування в ЗЦ/ЦЗО сертифікату на основі переданого запиту, сертифікат ЦСК, разом із ланцюгом сертифікатів вищестоящих органів, повинен бути зареєстрований на Сервері застосувань ЦСК.

Режим формування сертифіката ЦСК встановлюється в параметрах налаштування Сервера застосувань ЦСК перед генерацією ключів ЦСК.

Профілі сертифікатів, які використовуються у підсистемі управління ключами

У Таблиця 1 наведено перелік профілів сертифікатів ЦСК, які підтримуються за замовчуванням. За необхідністю, перелік може бути розширений.

Таблиця 1. Перелік профілей сертифікатів у ЦСК, за замовчуванням

Назва профілю	АРМ, у якому використовується	Призначення
Адміністратор реєстрації	АРМ адміністратора реєстрації	Використовується у ЦР. Підтвердження запитів на сертифікат, сформованих у процесі зміни ключів. Підтвердження запитів, засвідчених оператором реєстрації. Видача стартових сертифікатів. Засвідчення запитів на робочі ключі, згенерованих на АРМ адміністратора реєстрації. Підтвердження та формування запитів на блокування/відновлення/скасування сертифікатів. Запуск АРМ адміністратора реєстрації.
Віддалений адміністратор реєстрації	АРМ віддаленого адміністратора реєстрації	Використовується на віддалених ЦР. Підтвердження запитів на сертифікат, сформованих у процесі зміни ключів. Підтвердження запитів, засвідчених операторами реєстрації. Видача стартових сертифікатів. Засвідчення запитів на робочі ключі, згенерованих на АРМ віддаленого адміністратора реєстрації. Підтвердження та формування запитів на блокування/відновлення/скасування сертифікатів.

		Запуск АРМ віддаленого адміністратора реєстрації.
Оператор реєстрації	АРМ реєстратора Модуль генерації ключів	Використання у ЦР та територіально обумовлених ВПР. Засвідчення запитів на сертифікат, сформованих технологічним ПЗ. Видача стартових сертифікатів. Засвідчення запитів на робочі ключі, згенерованих на АРМ реєстратора та МГК. Засвідчення запитів на блокування/відновлення/скасування сертифікатів, сформованих на МГК. Повноваження ключів встановлюються на етапі генерації адміністратором безпеки та аудиту ЦСК. Запуск АРМ реєстратора.
Оператор ЦПД	АРМ оператора ЦПД	Використовується у ЦР. Формування запитів на блокування сертифікатів. Запуск АРМ оператора ЦПД.
Адміністратор сертифікації	АРМ адміністратора сертифікації ЦСК	Використовується у ЦР. Автентифікація на Сервері застосувань ЦСК. Автентифікація в АРМ адміністратора сертифікації ЦСК. Запуск сервера застосувань ЦСК. Запуск АРМ адміністратора сертифікації ЦСК.
Адміністратор безпеки центру сертифікації	АРМ адміністратора безпеки та аудиту ЦСК	Використовується у ЦСК. Автентифікація на сервері застосувань ЦСК. Автентифікація у АРМ адміністратора безпеки та аудиту ЦСК. Запуск Сервера застосувань ЦСК. Запуск АРМ адміністратора безпеки та аудиту ЦСК.
Адміністратор	АРМ системного адміністратора ЦСК	Використовується у ЦСК. Автентифікація на Сервері застосувань ЦСК. Автентифікація у АРМ системного адміністратора ЦСК. Запуск Сервера застосувань ЦСК. Запуск АРМ системного адміністратора.

Зауважимо, що у випадку необхідності, можуть бути додані додаткові профілі, а також відповідні фільтри.

Режими генерації ключів адміністраторів підсистеми управління ключами

У поточній версії системи ключі адміністраторів підсистеми управління ключами генеруються на АРМ адміністратора безпеки та аудиту ЦСК. При цьому, можуть бути згенеровані як робочі, так і стартові сертифікати адміністраторів.

При генерації робочих ключів власник може розпочати роботу одразу після встановлення відповідного програмного забезпечення.

При генерації стартових сертифікатів ключі адміністраторів підлягають зміні безпосередньо на відповідних робочих місцях. При цьому, стартовий ключ використовується тільки для

автентифікації запиту на сертифікат робочого ключа, а його власник може розпочати роботу тільки після отримання з ЦСК сертифіката робочого ключа.

Слід зауважити, що друга схема, хоч і більш складніша, однак надійніша, оскільки в ній застосовується принцип взаємної недовіри між адміністраторами безпеки і аудиту та іншими адміністраторами.

Технологія встановлення та ініціалізації роботи ЦСК

Передумови встановлення та ініціалізації роботи ЦСК

Програмне забезпечення сертифікації ключів розгортається в наступних приміщеннях:

- серверна – спеціальне приміщення, яке забезпечує надійний захист програмно-апаратних засобів та даних, в тому числі і МКМ;
- приміщення для робочих місць посадових осіб ЦСК;
- приміщення для мережевих компонентів – демілітаризована зона ЦСК (WWW-сервер, засоби мережевого захисту, телекомунікаційні засоби).

У серверній встановлюється обладнання для розгортання сервера застосувань та БД ЦСК.

У приміщенні для посадових осіб ЦСК розміщується обладнання для встановлення наступних програмних засобів:

- АРМ адміністратора безпеки та аудиту ЦСК;
- АРМ адміністратора сертифікації ЦСК;
- АРМ системного адміністратора ЦСК;
- Програмні засоби центру реєстрації;
- АРМ оператора ЦПД.

У приміщенні для мережевої компоненти ЦСК встановлюється обладнання для розгортання:

- LDAP-серверу;
- OCSP-серверу;
- TSP-серверу;
- CMP-серверу;
- WWW-серверу;
- Mail-серверу.

Порядок встановлення та ініціалізації роботи засобів ЦСК наступний [1]:

- Інсталяція та налаштування LDAP-сервера.
- Інсталяція та налаштування Сервера застосувань ЦСК.
- Ініціалізація системи внутрішньої автентифікації ЦСК.
- Генерація ключів сертифікації, формування запиту на сертифікат для надання у Центральний засвідчувальний орган чи виготовлення безпосередньо сертифікату ЦСК.
- Інсталяція АРМ адміністратора безпеки та аудиту ЦСК.
- Інсталяція АРМ адміністратора сертифікації ЦСК.
- Інсталяція АРМ системного адміністратора ЦСК.
- При отриманні сертифікату у вищестоячому засвідчувальному органі: отримання кореневого сертифікату та сертифікату ЦСК у вищестоячому засвідчувальному органі, завантаження вказаних вище сертифікатів у БД ЦСК та в LDAP-сервер;
- При передачі сертифікату TSA у вищестоячий засвідчувальний орган: отримання кореневого сертифікату та сертифікату TSA вищестоячому засвідчувальному органі, завантаження вказаних вище сертифікатів у БД ЦСК та в LDAP-сервер;
- Генерація ключів та формування сертифікатів для OCSP-сервера та TSP-сервера.
- Генерація необхідних сертифікатів адміністраторів реєстрації, операторів реєстрації та операторів ЦПД.
- Встановлення та ініціалізація роботи OCSP-сервера.
- Встановлення та ініціалізація роботи TSP-сервера.
- Встановлення та ініціалізація роботи CMP-сервера.
- Встановлення та ініціалізація роботи ЦР ЦСК.
- Встановлення та ініціалізація АРМ оператора ЦПД.

Ініціалізація системи внутрішньої автентифікації ЦСК, а також процедура генерації ключів сертифікації виконується безпосередньо на сервері застосувань за допомогою програми-

консолі сервера. Віддалений доступ до сервера застосувань (доступ з АРМ адміністратора безпеки та аудиту і АРМ адміністратора сертифікації) до повного виконання цих дій блокується.

Ключі та сертифікати системи внутрішньої автентифікації ЦСК

Функціонування системи внутрішньої автентифікації ЦСК забезпечують наступні ключі та сертифікати:

- Особистий ключ та сертифікат автентифікації адміністратора ЦСК (адміністратора ЦСК – будь-яка посадова особа ЦСК, але не адміністратор безпеки та аудиту чи адміністратор сертифікації, які можуть бути задіяні під час генерації ключів сертифікації).
- Особистий ключ та сертифікат автентифікації адміністратора безпеки та аудиту ЦСК.
- Особистий ключ та сертифікат автентифікації адміністратора сертифікації.
- Сертифікати відкритих ключів посадових осіб ЦСК обробляються за допомогою ключів сертифікації ЦСК.

Технологія ініціалізації системи внутрішньої автентифікації та генерації ключів сертифікації ЦСК

Генерація ключів сертифікації ЦСК виконується з консолі сервера застосувань в присутності адміністратора безпеки та аудиту ЦСК (кількість посадових осіб, які присутні під час генерації ключів, зазначається перед початком генерації ключів).

Послідовність дій при генерації ключів [3]:

- Генерації ключів сертифікації.
- Генерація особистих ключів автентифікації та формування відповідних сертифікатів посадовим особам ЦСК, які присутні у процесі ініціалізації системи внутрішньої автентифікації ЦСК та генерації ключів сертифікації.

Ключі сертифікації ЦСК генеруються і зберігаються:

- У файловому НКІ. Ключ сертифікації ЦСК зашифровується та у зашифрованому вигляді у складі файлового контейнера ключів ЦСК записується на жорсткий диск Сервера застосувань ЦСК.
- У захищеному НКІ.
- У МКМ.

Доступ до ключа сертифікації ключів ЦСК розподіляється між всіма адміністраторами – учасниками процедури генерації ключів сертифікації ЦСК.

Кожна посадова особа, яка приймає участь в генерації ключів, отримує НКІ, на якому будуть збережені:

- Особистий ключ автентифікації посадової особи.
- Зашифрована частина ключа шифрування для захисту особистого ключа сертифікації ЦСК.

При генерації ключів у самопідписаному режимі, сертифікат відкритого ключа ЦСК формується безпосередньо у момент генерації ключів та зберігається у БД ЦСК та LDAP-каталог.

При генерації ключів у режимі під керівництвом ЗЦ/ЦЗО, відкритий ключ у вигляді файлу-запиту на сертифікат у форматі PKCS#10 записується на НКІ (носії із запитом надається у ЗЦ/ЦЗО для формування сертифікату ЦСК).

Сертифікати відкритого ключа автентифікації зберігаються на НКІ посадових осіб та у БД ЦСК на жорсткому диску Сервера застосувань ЦСК.

У подальшому, особисті ключі автентифікації для другого адміністратора безпеки та аудиту та адміністраторів сертифікації, перший адміністратор безпеки та аудиту генерує зі свого робочого місця – АРМ адміністратора безпеки та аудиту. З цього ж робочого місця виконуються всі дії, пов'язані із формуванням сертифікатів автентифікації, збереженням цих сертифікатів у БД Сервера застосувань ЦСК, а також особисті НКІ посадових осіб ЦСК.

Технологія завантаження кореневого сертифіката та сертифіката ЦСК

Дана процедура виконується тільки у режимі роботи під керівництвом вищестоячого засвідчувального органу.

Завантаження кореневого сертифіката та сертифіката ЦСК виконується після їх отримання з ЦЦ/ЦЗО.

Дана процедура виконується адміністратором безпеки та аудиту ЦСК з консолі сервера застосувань. У процесі завантаження, вказані сертифікати записуються у НКІ для ключів ЦСК, у БД даних ЦСК та в LDAP-каталог.

Технологія доступу та обміну даними між АРМ посадових осіб та сервером застосувань ЦСК

Підключення АРМ адміністратора безпеки та аудиту (адміністратора сертифікації) до сервера застосувань ЦСК виконується за наступною технологією.

АРМ адміністратор безпеки та аудиту (адміністратора сертифікації)

У процесі ініціалізації з'єднання з Сервером застосувань ЦСК, генерує та зберігає у пам'яті тимчасову пару ключів Діффі-Хелмана – особистий та відкритий.

Формує блок автентифікаційних даних:

- Ідентифікатор ключів автентифікації адміністратора.
- Відкритий ключ Діффі-Хелмана.
- Службові дані.

Підписує блок автентифікаційних даних за допомогою особистого ключа автентифікації адміністратора.

Передає підписаний блок автентифікаційних даних на сервери.

Сервер застосувань ЦСК

Приймає підписаний блок автентифікаційних даних.

За ідентифікатором визначає повноваження доступу до задач та даних, відшукує та автентифікує відповідний сертифікат автентифікації.

Відкритим ключем із сертифікату перевіряє ЕП автентифікаційних даних.

У випадку успіху всіх перевірок генерує та зберігає у пам'ять свою пару параметрів (особистий та відкритий) Діффі-Хелмана.

Відкритий параметр передає на адресу АРМ адміністратора, як відповідь запиту на з'єднання.

АРМ адміністратора безпеки та аудиту (адміністратора сертифікації)

Приймає та зберігає у пам'яті відкритий ключ Діффі-Хелмана, сформований на стороні сервера.

Після виконання вищевказаних дій весь обмін даними між АРМ адміністратора безпеки та аудиту (адміністратора сертифікації) та сервером застосувань ЦСК виконується у зашифрованому вигляді. Ключ шифрування формується за протоколом Діффі-Хелмана.

Встановлення та ініціалізація роботи засобами ЦР

При розгортанні ЦР ЦСК програмні засоби ЦР встановлюються у приміщенні для посадових осіб ЦСК, АРМ оператора ЦПД встановлюється у відповідному приміщенні.

Порядок встановлення та ініціалізація роботи вказаних ПЗ:

- Інсталяція засобів сервера БД ЦР та розгортання БД ЦР.
- Отримання адміністратором реєстрації у адміністраторів безпеки та аудиту ЦСК НКІ, які містять кореневий сертифікат та робочі/стартові ключів адміністратора реєстрації;
- Інсталяція АРМ адміністратора реєстрації.
- У випадку застосування стартового сертифікату, генерація робочих ключів, формування та відправка запиту на сертифікат робочого ключа адміністратора реєстрації.
- Отримання та збереження сертифікатів робочих ключів адміністратора реєстрації.
- Інсталяція АРМ реєстрації.
- Отримання оператором реєстрації в адміністратора безпеки та аудиту ЦСК НКІ, які містять кореневий сертифікат та робочі/стартові ключі оператора реєстрації;

- У випадку застосування стартового сертифікату, генерації робочих ключів, формування та відправка запиту на сертифікат робочого ключа оператора реєстрації.
- Отримання та збереження запиту на сертифікат робочого ключа оператора реєстрації.
- Отримання та збереження сертифікатів оператора реєстрації.
- Інсталяція АРМ оператора ЦПД.
- Отримання оператором ЦПД у адміністратора безпеки та аудиту ЦСК НКІ, котрі містять кореневий сертифікат та робочі/стартові ключі оператора ЦПД.
- Генерація робочих ключів, формування та відправка запиту на сертифікат робочого ключа оператора ЦПД.
- Отримання та збереження сертифікатів оператора ЦПД.
- Інсталяція комунікаційного модуля.
- Інсталяція модуля генерації ключів користувача на відокремлену робочу станцію у ЦР.

Технологія взаємодії засобами підсистеми сертифікації при розгортанні ЦР ЦСК

Взаємодія засобів підсистеми сертифікації при розгортанні ЦР ЦСК, для всіх операторів засобами адміністрування ключів ЦР:

- Адміністраторів реєстрації.
- Віддалених адміністраторів реєстрації.
- Операторів реєстрації.
- Операторів ЦПД.

виконується за наступною схожою технологією.

При генерації оператору робочих ключів

У даному режимі робочі ключі відповідного профілю генеруються на АРМ адміністратора безпеки та аудиту ЦСК.

У процесі генерації адміністратор безпеки та аудиту ЦСК заповнює необхідні анкетні дані та формує ключі на НКІ, який містить робочі особисті ключі адміністратора, сертифікат відкритого ключа та ланцюг сертифікатів ЦСК.

Отримав даний НКІ, адміністратор (оператор) може одразу приступати до роботи.

При генерації оператору стартових ключів

У даному режимі на АРМ адміністратора безпеки та аудиту ЦСК генеруються стартові ключі відповідного профілю.

У процесі генерації адміністратор безпеки та аудиту ЦСК заповнює необхідні анкетні дані та формує ключі на НКІ, які містять стартові секретні ключі оператора, стартовий сертифікат відкритого ключа та ланцюг сертифікатів ЦСК.

Отримав даний контейнер, оператора реєстрації за допомогою відповідного АРМ (адміністратора реєстрації, реєстратора чи оператора ЦПД) виконує зміну стартових ключів. У процесі зміни, засоби адміністрування формують запити на сертифікат робочих ключів у форматі PKCS#7, підписаний стартовим ключем, згенерованим адміністратором безпеки та аудиту ЦСК.

Даний запит відправляється на ЦСК електронною поштою. Сервер застосувань ЦСК, у процесі зміни, перевіряє автентичність запиту та зберігає його у БД ЦСК.

Засвідчення даного запиту здійснюється на сервері застосувань ЦСК по команді адміністратора безпеки та аудиту ЦСК. При цьому сервер застосувань ЦСК формує сертифікат, який буде надісланий на адресу відповідного АРМ електронною поштою.

Прийом сертифікату забезпечує відповідний АРМ, який після перевірки автентичності сертифікату, зберігає його у БД ЦР та в НКІ власника, та після цього, вводить у дію робочі ключі адміністратора.

Слід зауважити, що, оскільки у АРМ реєстратора відсутній інтерфейс до електронної пошти, відправлення запитів на сертифікат операторів реєстрації та прийом сертифікатів здійснює функціонуючий у рамках ЦР АРМ адміністратора реєстрації.

Технологія встановлення та ініціалізації роботи ВПР

Передумови встановлення та ініціалізації роботи ВПР

Для наближення послуг по видачі сертифікатів користувачам, які територіально віддалені від ЦСК, розгортається ВПР. ВПР у складі ПЗ, а також виконуючи функції ідентичні ЦР, який функціонує у складі ЦСК.

ВПР розгортається у приміщенні, яке з одного боку, забезпечує захист від НСД, а з іншого – дозволяє вести прийом користувачів, які видають сертифікати. У приміщенні ВПР розміщується обладнання для встановлення наступних ПЗ:

- АРМ адміністратора реєстрації.
- АРМ віддаленого адміністратора реєстрації.
- АРМ реєстратора.
- Сервер БД ВПР.
- Резервна БД ВПР.
- Локальний LDAP-сервер (зберігає сертифікати, видані виключно даними ВПР).
- Модуль генерації ключів користувача.

Порядок встановлення та ініціалізації роботи ВПР наступний:

- Інсталяція засобів сервера БД ЦР розгортання самої БД ЦР.
- Інсталяція та налаштування LDAP-сервера ЦР (за необхідності).
- Отримання адміністратором реєстрації у адміністратора безпеки та аудиту ЦСК НКІ, які містять кореневий сертифікат та робочі/стартові ключі адміністратора реєстрації;
- Інсталяція АРМ адміністратора реєстрації.
- У випадку використання стартового сертифікату, генерація робочих ключів, формування та відправка запиту на сертифікат робочого ключа адміністратора реєстрації.
- Отримання та збереження сертифікатів робочих ключів адміністратора реєстрації.
- Отримання та збереження сертифікату адміністратора реєстрації.

Технологія взаємодії підсистеми сертифікації при розгортанні ВПР

Взаємодія засобів підсистеми сертифікації при розгортанні Відокремлених ПР виконується за технологією описаною вище. Після успішного виконання цих дій ініціалізація ВПР вважається завершеною та дозволяється обслуговування користувачів.

Технологія управління ключами та сертифікатами користувачів

Загальна інформація

Підсистема сертифікації надає наступні можливості з обслуговування користувачів з метою отримання ними сертифікатів відкритих ключів:

- Генерація ключів користувачів та видача відповідних сертифікатів безпосередньо у ЦР, не залежить від того, де ЦР розміщений – у рамках ЦСК чи це ВПР;
- Самостійне управління ключами та сертифікатами (генерація робочих ключів та отримання відповідних сертифікатів).
- Генерація ключів користувачів за допомогою технологічного ПЗ.

Генерація ключів користувачів безпосередньо у ЦР

Генерацію ключів користувачів безпосередньо у ЦР забезпечують засоби АРМ адміністратора реєстрації, АРМ віддаленого адміністратора реєстрації та АРМ реєстратора. При цьому користувачу можуть генеруватися, як робочі, так і стартові ключі.

Генерація робочих ключів користувачів

При генерації робочих ключів користувача у НКІ генеруються особисті ключі власника, запит на сертифікат відкритих ключів та кореневий сертифікат ЦСК. Одночасно у ЦСК буде надіслано запит на сертифікат власника. ЦСК, після засвідчення даного запиту. Розміщує відповідний сертифікат у LDAP-каталозі.

Реєстрація даного сертифікату в НКІ та введення у дію особистих ключів власника здійснюють бібліотеки криптофункцій, функціонуючи у рамках відповідного технологічного ПЗ.

Генерація стартових ключів користувачів

При генерації стартових ключів користувача у НКІ генеруються стартові особисті ключі власника, стартові сертифікати відкритих ключів та ланцюг сертифікатів ЦСК.

Власник стартових ключів здійснює їх зміну за допомогою бібліотек криптографічних функцій, чи засобами МГК.

При зміні стартових ключів за допомогою бібліотек криптографічних функцій, формується запит на сертифікат робочих ключів у форматі PKCS#7, підписаний стартовим ключем, де технологічне ПЗ, під керівництвом якого функціонують бібліотеки криптографічних функцій, повинні надсилатися у вигляді файлу до АРМ адміністратора реєстрації. АРМ адміністратора реєстрації перевіряє автентичність даного запиту та зберігає його у БД ЦР. Після того, як адміністратор реєстрації засвідчить даний запит свого ЕП, він буде надісланий електронною поштою на сервер застосувань ЦСК.

Сервер застосувань ЦСК, після засвідчення даного запиту, розмістить відповідний сертифікат у LDAP-каталозі.

Реєстрацію сертифіката робочих ключів у НКІ та введення у дію особистих ключів власника здійснюють бібліотеки криптографічних функцій, які функціонують у рамках відповідного технологічного ПЗ.

Крім цього, користувач може здійснити зміну стартових ключів безпосередньо у ЦР, використовуючи МГК. МГК, який може бути встановлений у рамках цих ЦР. Робоча станція на якій розгортається та функціонує ПЗ МГК, повинна бути фізично відділена від локальної мережі ЦР.

Самостійне управління ключами та сертифікатами

Самостійне управління ключами та сертифікатами користувачів забезпечує МГК. ПЗ МГК може видаватися користувачам на ЦР. Інший варіант доступу користувачів до МГК – його завантаження з публічного Web-сервера ЦСК.

МГК повинен встановлюватися на робочі станції, які мають засоби захисту від НСД.

Порядок встановлення та ініціалізації роботи МГК буде наступним:

- Отримання користувачем на ЦР інсталяційного пакета МГК (може не виконуватись за наявності двох варіантів доступу до засобів МГК);
- Отримання користувачем у адміністратора/оператора реєстрації НКІ, який містить кореневий сертифікат та робочі/стартові ключі;
- Інсталяція МГК.
- У випадку використання стартових ключів, генерація робочих ключів, формування та відправка запиту на сертифікат робочого ключа.
- Отримання та збереження сертифікатів робочих ключів.

Генерація ключів користувачів за допомогою технологічного ПЗ

Генерація ключів користувачів за допомогою технологічного ПЗ здійснюється за допомогою бібліотек криптографічних функцій. У процесі генерації ключів технологічне ПЗ повинно здійснювати правильне заповнення необхідних полів запиту на сертифікат, після генерації ключів надійде запит на сертифікат у форматі PKCS#10 до ЦР.

Комунікаційний модуль імпортує запит у форматі PKCS#10, після перевірки даного запиту, збереже його у БД ЦР.

Засвідчення запитів на сертифікат формату PKCS#10 здійснюється на АРМ реєстратора при отриманні ним інформації, який підтверджує автентичність даних у прийнятих запитах, наприклад, паперового засвідчення, відповідного запиту на сертифікат, завіреного рукописного підпису власника.

Після засвідчення запиту на сертифікат формату PKCS#10 оператором реєстрації, даний запит повинен бути засвідчений адміністратором реєстрації. Після того, як адміністратор реєстрації засвідчить запит своїм ЕП, він буде відправлений електронною поштою на Сервер застосувань ЦСК.

Сервер застосувань ЦСК, після засвідчення даного запиту, розмістить відповідний сертифікат у БД ЦСК та у LDAP-каталозі.

Реєстрація сертифіката робочих ключів у НКІ та введення у дію особистих ключів власника здійснюють бібліотеки криптографічних функцій, які функціонують у рамках відповідного технологічного ПЗ.

Планова зміна ключів та сертифікатів

Планова зміна ключів та сертифікатів співробітників ЦСК

Взаємодія засобів підсистеми управління ключами та сертифікатами при плановій зміні ключів та сертифікатів адміністратора реєстрації та оператора ЦПД виконуються за наступною технологією.

Засоби адміністрування ключів ЦР (АРМ адміністратора реєстрації, АРМ реєстратора та АРМ оператора ЦПД) забезпечують автоматичну перевірку строку дії ключів по даті у діючому сертифікаті (при кожному старті чи у випадку цілодобової роботи залишилось 14 днів чи менше, адміністратора (оператора) видається попередження про необхідність виконання процедури зміни ключів. По команді адміністратора (оператора) засобами АРМ здійснюють генерацію нових особистих чи відкритих ключів посадових осіб. Черговий особистий ключ зберігається у НКІ, формується запит на сертифікат чергового відкритого ключа.

Далі виконуються дії, які аналогічні діям описаних у підрозділі.

Відмінність у наступному:

- При формуванні PKCS#7-запиту, підписання виконується на час генерації особистим ключем власника.
- На ЦСК перевіряється автентичність PKCS#7-запиту на отримання чергового сертифікату виконується відкритим ключем діючим сертифікатом адміністратора власника.

Зміна ключів та сертифікатів користувача

Взаємодія засобів підсистеми сертифікації при плановій зміні ключів та сертифікатів користувача виконується за наступною технологією.

Перевірка строку дії ключа та сертифікату користувача забезпечується засобами бібліотек криптографічних функцій. Дана перевірка виконується при ініціалізації бібліотек, яка супроводжується введенням особистого ключа та перевіркою відповідного сертифікату. Програма, яка керує роботою бібліотек, отримує інформацію про те, що до закінчення терміну дії ключів залишилось N днів чи менше (N – налаштовуваний параметр) та передає її користувачу.

Користувач може здійснити зміну ключів самостійно за допомогою МГК чи відповідних процедур бібліотек криптографічних функцій. В останньому випадку зміна ключів повинна підтримуватися програмою, яка керує роботою бібліотек.

Зміна ключів за допомогою МГК виконується за наступною технологією. За командою користувача засобами МГК здійснюють генерацію нових особистих та відкритих ключів. Чергові особисті ключі зберігаються у НКІ користувача, формується запит на сертифікат чергового відкритого ключа.

Далі, виконуються дії, які аналогічні викладеним раніше. Відмінність полягає у наступному:

- При формуванні PKCS#7-запиту, підписання виконується чинним на момент генерації особистим ключем користувача.
- На Центрі реєстрації перевірка автентичності PKCS#7-запиту на отримання чергового сертифіката користувача здійснюється відкритим ключем з чинного сертифіката, який належить даному користувачу.

Технологія функціонування засобів підсистеми сертифікації при скасуванні, блокуванні та відновленні дії сертифікатів

Скасування, блокування та відновлення дії сертифікатів виконується виключно ЦСК. ЦСК інформує користувачів про їх дії шляхом формування, публікації та розсилки СВС (та дельта-СВС).

Дії відкликаноного сертифікату не відновлюються.

Скасування сертифікатів виконується:

- Адміністратором сертифікації на основі рішення адміністрації ЦСК, якому із довірених джерел стало відомо про компрометацію відповідного особистого ключа.
- Адміністратором реєстрації чи адміністратором ЦПД на основі заяви власника сертифіката після його ідентифікації.
- Адміністратором реєстрації на основі запиту на скасування сертифіката, який сформований власником, після перевірки автентичності даного запиту.
- Власником сертифікату з використанням технологічного ПЗ формується запит на блокування чи відкликання сертифікату, який надсилається до ЦР.

Відкликаний сертифікат застосовується для перевірки ЕП з наступним обмеженням:

- ЕП вважається дійсним, якщо дата та час формування ЕП менше відповідної дати та часу скасування сертифікату (після відкликання сертифікату відповідний особистий ключ не може бути використаний для виконання процедури формування ЕП).
- Дію заблокованого сертифіката може бути відновлено в рамках загального строку дії даного сертифіката.

Блокування дії сертифікату здійснюється:

- Адміністратором реєстрації, чи оператором ЦПД на підставі заяви власника сертифіката після його ідентифікації.
- Адміністратором реєстрації на підставі запиту на блокування сертифікату, сформованого власником, після перевірки автентичності цього запиту.
- Власником сертифікату з використанням технологічного ПЗ формується запит на блокування чи відкликання сертифікату, який надсилається до ЦР.

Відновлення дії заблокованого сертифікату виконується:

- Адміністратором реєстрації чи адміністратором ЦПД на основі заяви власника сертифікату після його ідентифікації;
- На основі рішення адміністрації ЦСК, якщо інформація про можливість компрометації відповідного особистого ключа не підтверджена.
- Сертифікат, дія якого заблокована, застосовується для перевірки ЕП з наступними обмеженнями:
 - ЕП вважається дійсним, лише у випадку, якщо дата та час формування ЕП менше відповідної дати та часу блокування дії сертифікату (особистий ключ, який відповідає заблокованому сертифікату, не може бути використаний для виконання процедури формування ЕП).

Сертифікат, дію якого відновлено, застосовується для перевірки ЕП з наступними обмеженнями:

- ЕП вважається дійсним, у випадку, якщо дата та час формування ЕП менше відповідної дати та часу блокування дії сертифіката.
- ЕП вважається дійсним у випадку, якщо дата та час формування ЕП більше відповідної дати та часу відновлення дії сертифіката.
- За наявності електронної позначки часу підпису, яка свідчить про час створення ЕП.

Технологія формування, збереження та розсилка СВС

Формування, збереження та розсилка СВС здійснюється за наступною технологією.

Сервер застосувань ЦСК (за командою адміністратора сертифікації чи автоматично) забезпечує виконання наступних дій:

- Формування СВС (та дельта-СВС).
- Збереження СВС (та дельта-СВС) у БД.
- Збереження (публікація) СВС у LDAP-каталозі.
- Передача СВС (та дельта-СВС) серверу OCSP.
- Запис СВС (та дельта-СВС) у спеціальний каталог для організації його доставки користувачам через Web-сайт ЦСК.
- Розсилка СВС (та дельта-СВС) електронною поштою у відповідності зі спеціальним реєстром отримувачів СВС.
- Протоколювання виконаних дій.

АРМ адміністратора реєстрації забезпечує виконання наступних дій:

- У випадку відсутності СВС (та дельта-СВС) у БД ЦР, здійснюється його пошук у LDAP-каталозі з наступним завантаженням.
- Прийом отриманого електронною поштою СВС (та дельта-СВС).
- Автентифікація завантаженого СВС (та дельта-СВС) за допомогою сертифікату ЦСК.
- Збереження отриманого та перевіреного СВС (та дельта-СВС) у БД ЦР.
- Збереження СВС (та дельта-СВС) у спеціальному каталозі для забезпечення доступу до нього засобів криптографічного захисту даних;
- Розсилка СВС (та дельта-СВС) електронною поштою у відповідності зі спеціальним реєстром отримувачів СВС (та дельта-СВС).
- Протоколювання виконаних дій.

Технологія скасування, блокування та відновлення дії сертифікатів з адміністратором реєстрації (оператором ЦПД)

Скасування, блокування та відновлення сертифікатів з адміністратором реєстрації (оператором ЦПД) виконується за наступною технологією.

АРМ адміністратора реєстрації (АРМ оператора ЦПД) забезпечує виконання наступних дій:

- Формування підписаного ЕП адміністратора реєстрації (оператора ЦПД) запиту на скасування/блокування/відновлення дії сертифікату (PKCS#7).
- Формування поштового повідомлення та приєднання до нього файлу-запиту на скасування/відновлення/блокування з подальшим відправленням.
- Збереження запиту (PKCS#7) на скасування/відновлення/блокування у БД ЦР зі статусом «відправлено».
- Протоколювання виконаних дій.

Програмні засоби сертифікації ключів

Сервер застосувань ЦСК забезпечує виконання наступних дій:

- Прийом поштових повідомлень із запитом на скасування/відновлення/блокування.
- Перевірка автентичності запиту (PKCS#7) на скасування/відновлення/блокування (виконується за допомогою сертифікату адміністратора реєстрації чи оператора ЦПД).
- Збереження запиту (PKCS#7) на скасування/відновлення/блокування у БД ЦСК.
- Формування квитанції про прийом запиту, з подальшим її відправленням електронною поштою на адресу відправника запиту.
- Формування, збереження та розсилка СВС (та дельта-СВС).
- Протоколювання виконаних дій.

АРМ адміністратора реєстрації (АРМ оператора ЦПД) забезпечує виконання наступних дій:

- Обробка квитанції та надання збереженому запиту на скасування/відновлення/блокування статусу «прийнятий ЦСК на обробку».
- Протоколювання виконаних дій.

Центр сертифікації ключів

АРМ адміністратора сертифікації (через сервер застосувань ЦСК) забезпечує виконання наступних дій:

- Контроль наявності у БД ЦСК запитів, які підлягають обробці.
- Вибір із БД PKCS#7-запиту на скасування/відновлення/блокування.
- Перевірка автентифікації запиту (PKCS#7) на скасування/відновлення/блокування (виконується за допомогою сертифікату ЦР).
- Підтвердження можливості обробки запиту з метою отримання СВС (та дельта-СВС).
- Протоколювання виконаних дій.

Сервер застосувань ЦСК забезпечує наступні дії:

- Вибір із БД перевіреного адміністратором сертифікації запиту скасування/відновлення/блокування.
- Формування, збереження та розсилка СВС (та дельта-СВС).
- Протоколювання виконаних дій.

Технологія скасування та блокування дії сертифікатів на основі запитів користувачів

Скасування та блокування дії сертифікатів на основі запитів користувачів виконуються за наступною технологією.

МГК забезпечує виконання наступних дій:

- Формування по команді користувача, підписаного ЕП користувача, запиту PKCS#7 на скасування/блокування дії сертифіката.
- Передача поштового повідомлення із запитом у ЦР.
- Збереження запиту PKCS#7 на скасування/блокування у БД МГК зі статусом «відправлено».
- Протоколювання виконаних дій.

АРМ адміністратора реєстрації забезпечує виконання наступних дій:

- Прийом та перевірка автентифікації запиту PKCS#7 на скасування/блокування (виконується за допомогою сертифікату користувача).
- Формування квитанції про прийом запиту та передачі поштового повідомлення з квитанцією на адресу користувача.
- Засвідчення ЕП адміністратора реєстрації запиту PKCS#7 на скасування/блокування дії сертифіката користувача.
- Передача поштового повідомлення із запитом у ЦСК.
- Збереження запиту PKCS#7 на скасування/блокування у БД ЦР зі статусом «відправлено».
- Протоколювання виконаних дій.

Далі виконуються дії, викладені у пунктах 2, 3, 4 підрозділу 3.5.2.

Примітка

Технологія, описана у даному розділі, не застосовується для відновлення дій сертифіката. Для відновлення дій цього сертифіката користувач особисто звертається у ЦР чи у ВПР ЦСК. Відповідний адміністратор реєстрації чи оператор ЦПД після ідентифікації користувача ініціює відновлення дії його сертифікату.

Технологія функціонування підсистеми криптографічного захисту даних

Функції підсистеми криптографічного захисту, реалізовані у наступних бібліотеках:

- Бібліотека криптографічних функцій для підсистеми Win32.
- Бібліотека криптографічних функцій Java.
- Бібліотека функцій реєстрації для підсистеми Win32.

Технологія функціонування бібліотек криптографічних функцій

Криптографічні перетворення

Перевірка автентичності та статусу сертифіката

При перевірці автентичності та статусу сертифіката бібліотеки криптографічних функцій виконують наступні дії:

- За ідентифікатором (надається бібліотеці, яка програмою викликає безпосередньо у складі ЕП чи у складі службового блоку даних, який формується при виконанні криптографічних перетворень) відшукується та завантажується сертифікат користувача.
Пошук може виконуватися:
 - У НКІ, на носії користувача.
 - У персональній БД бібліотек.
 - У БД ЦР.
 - У LDAP-каталозі (за протоколом LDAP).
 - За запитом до CMP-серверу.
 - За запитом до OCSP-серверу.
- За ідентифікатором (знаходиться у сертифікатах користувачів) відшукується та завантажує старші сертифікати (сертифікат ЦСК, кореневий сертифікат) та вибудовується ланцюг сертифікатів: сертифікат(и) користувача – сертифікати ЦСК – кореневий сертифікат.
- Перевіряється автентичність кореневого сертифікату (кореневий сертифікат – самопідписаний).
- За допомогою кореневого сертифікату перевіряється автентичність сертифікату ЦСК (строк дії кореневого сертифікату не повинен бути закінчений на момент формування ЕП сертифікату ЦСК).
- За допомогою сертифікату ЦСК перевіряється автентичність сертифікату користувача (строк дії сертифікату ЦСК не повинен бути закінчений на момент формування ЕП сертифікату користувача).
- Якщо всі перевірки успішні, перевіряються повноваження сертифікату користувача на виконання операції (ЕП та/чи зашифрування).

Перевіряється статус сертифікату на час виконання операції:

- Під час формування ЕП та виконання зашифрування – сертифікат повинен бути чинним на поточний час.
- При перевірці ЕП – сертифікат повинен бути чинним на дату формування ЕП.
- Для операції розшифрування – сертифікат повинен бути чинним на дату виконання процедури зашифрування.

Статус сертифікату перевіряється шляхом запиту на сервер OCSP чи CBC – на час виконання операції, сертифікат не повинен бути відкликаний чи блокований.

Вказані процедури виконуються бібліотекою безумовно та автоматично при кожній дії із сертифікатом.

Якщо контроль статусу сертифікатів виконується за CBC, файл CBC постійно контролюється на актуальність. При зміні файлу CBC він завантажується бібліотекою, здійснюється перевірка його цілісності та автентичності.

Формування ЕП

Процес формування ЕП ініціюється програмою, яка викликає. Для формування ЕП використовуються особистий ключ, який під час ініціалізації завантажується у пам'ять. Блок даних, який вимагає підпис, надається бібліотекою програми, яка викликає.

Бібліотека виконує наступні дії:

- завантаження сертифікату, який відповідає введеному особистому ключу;
- перевірка автентичності та статусу завантаженого сертифіката;
- гешування даних, які підписуються;
- виділення у пам'ять буфера обміну для ЕП;
- формування ЕП та запис її у виділений буфер;
- повернення сформованого ЕП програмою, яка викликає.

ЕП у своєму складі містить:

- власне ЕП даних;
- дату, час формування ЕП;
- ідентифікатор сертифікату, який необхідний для перевірки ЕП;
- допоміжні дані.

Перевірка ЕП

Процес перевірки ЕП ініціюється програмою, яка викликає. Блок даних та відповідний йому ЕП, який вимагає перевірки, який надається бібліотеці програмою, яка викликає.

Бібліотека виконує наступні дії:

- пошук та завантаження сертифікату, необхідного для перевірки ЕП (за ідентифікатором з ЕП);
- перевірка автентичності завантаженого сертифікату та його статус на час формування ЕП;
- перевірка ЕП за допомогою відкритого ключа із завантаженого сертифікату;
- повернення програмі результату перевірки ЕП.

Технологія ключів узгодження секрету для зашифровування даних

Ключі узгодження секрету

При виконанні кожної процедури зашифровування даних використовуються разові ключі зашифрування, які генеруються бібліотекою безпосередньо у процесі виконання даної процедури.

При зашифруванні для ключів зв'язку зашифрування даних, бібліотека виконує наступні дії:

- За ідентифікатором отримувача зашифрованих даних (передається програмою, яка викликає) відшукує та завантажує сертифікат, який належить отримувачу.
- Перевіряє автентичність та статус завантаженого сертифікату.
- Із перевіреного сертифікату обирає відкритий параметр Діффі-Хелмана.
- Використовуючи секретний параметр Діффі-Хелмана, який завантажується під час ініціалізації разом із особистим ключем ЕП та відкритий параметр із сертифіката отримувача, обробляє загальний для зашифрування, особистий ключ Діффі-Хелмана.
- За допомогою отриманого ключа виконується процедура зашифрування даних за допомогою блочного симетричного шифру у відповідному режимі.

При виконанні процедури розшифрування у процесі ключів зв'язку зашифрованих даних, бібліотека виконує наступні дії:

- За ідентифікатором отримувача, який знаходиться у заголовку зашифрованих даних (надається програмою, яка викликає), відшукує та завантажує сертифікат отримувача.
- Перевіряє автентичність та статус завантаженого сертифіката.
- Використовуючи особистий ключ Діффі-Хелмана та відкритий ключ із сертифіката відправника, узгоджує спільний секрет для шифрування за допомогою блочного симетричного шифру.

- За допомогою отриманого ключа виконується процедура розшифрування даних за допомогою блочного симетричного шифру у відповідному режимі.

Отриманий таким чином ключ зашифрування використовується бібліотекою під час виконання процедури розшифрування даних.

Зашифрування даних

Процес зашифрування даних ініціюється програмою, яка викликає, надає бібліотеці дані для зашифрування даних.

При зашифруванні, бібліотека виконує наступні дії:

- Для кожного з отримувачів виконує процедуру узгодження ключа зашифрованих даних.
- Формує конверт PKCS#7 зашифрованих даних у складі.
- Виконує зашифровування даних.

Розшифрування даних

Процес розшифрування даних ініціюється програмою, яка викликає і надає бібліотеку зашифрування даних та відповідний їй конверт PKCS#7 зашифрованих даних.

При розшифруванні, бібліотека виконує наступні дії:

- Для кожного із отримувачів виконує процедуру узгодження ключа зашифрованих даних.
- Формує конверт PKCS#7 зашифрованих даних у складі.
- Виконує розшифровування даних.

Зміна ключів та сертифікатів

Програма, яка викликає при ініціалізації бібліотеки надає їй дані, на основі яких бібліотека робить висновок про необхідність виконання процедури зміни поточних ключів користувача. Бібліотека, після аналізу цих даних, надає програмі, яка викликає відповідну інформацію. Після отримання інформації про необхідність зміни ключів, програма, яка викликає, інформує про це користувача і за командою ініціює процедуру зміни, шляхом виклику відповідної функції бібліотеки.

Бібліотека виконує генерацію ключів, зберігає особисті ключі у НКІ та формує запит на сертифікацію нових відкритих ключів. Згенерований бібліотекою запит на сертифікацію нових відкритих ключів записується у ключовий контейнер та повертається програмі, яка викликає і забезпечує його відправлення у ЦСК.

Отримання нового сертифіката та введення у дію ключів виконується за наступною технологією. При кожному старті, під час ініціалізації бібліотека перевіряє наявність у НКІ ключів, які вимагають введення у дію.

Якщо особистий ключ та запит на сертифікат відкритого ключа знаходиться у НКІ, бібліотека виконує наступні дії:

- Встановлює з'єднання з LDAP-сервером.
- Отримує та перевіряє автентичність, статус сертифікату.
- При позитивному результаті перевірки зберігає сертифікат у НКІ замість відповідного запиту.
- Перевіряє строк введення у дію сертифіката, якщо такий настав, вводять у дію нові ключі.

Про факт введення у дію ключів, бібліотека інформує програму, яка викликає.

Робота з електронними позначками часу

Формування запиту на електронну позначку часу

Процес формування запиту на електронну позначку часу ініціюється програмою, яка викликається і надає бібліотеці дані для формування запиту.

При формуванні запиту на електронну позначку часу бібліотека виконує наступні дії:

- Гешування даних, для яких формується електронна позначка часу.

- Формування запиту на електронну позначку часу у форматі PKCS#7 (ЕП створюється особистим ключем, який був введений під час ініціалізації бібліотеки).
- Інтерактивний режим роботи з електронними позначками часу:
 - Встановлення з'єднання з сервером TSP та передача йому сформованого запиту.
 - Очікування отримання електронної позначки часу.

Отримання відповіді на запит електронну позначки часу

При роботі із сервером TSP отримання електронної позначки часу здійснюється в рамках однієї транзакції.

Під час прийому електронної позначки часу бібліотека виконує наступні дії:

- За ідентифікатором видавця, який знаходиться у позначці, відшукує та завантажує сертифікат видавця.
- Перевіряє автентичність та статус завантаженого сертифікату.
- Перевіряє ЕП видавця під електронною позначкою часу.
- Надає програмі, яка викликає:
 - Перевірену електронну позначку часу.
 - Геш-функцію даних перевірених електронною позначкою часу.
 - Інформацію про час видачі електронної позначки часу та про її видавця.

Перевірка автентичності електронної позначки часу, яка зберігається разом з даними

Процес перевірки автентичності електронної позначки часу ініціюється програмою, яка викликається та надається бібліотеці:

- Електронну позначку часу.
- Дані, для яких призначена та разом із якими зберігається електронна позначка часу.

Під час перевірки автентичності електронної позначки часу, бібліотека виконує наступні дії:

- Гешування даних, які відповідають електронній позначці часу, яка перевіряється.
- Побітне звірення сформованої геш-функції з геш-функцією електронної позначки часу, яка перевіряється (таким чином, перевіряється відповідність даних та електронної позначки часу).
- Пошук та завантаження сертифікату видавця позначки (за ідентифікатором видавця, який знаходиться у позначці).
- Перевірка автентичності та статусу завантаженого сертифікату;
- Перевірка ЕП видавця під електронною позначкою часу.
- Повернення програмі, яка викликає:
 - Результат перевірки електронної позначки часу.
 - Інформацію про час видачі електронної позначки часу та її видавця.

Технологія функціонування бібліотек функцій реєстрації

Бібліотека призначення для побудови на сторонні застосування, для можливості генерації стартових чи робочих ключів, формування заявок на видачу сертифіката, формування заявок на блокування та відновлення сертифікатів, формування заявок на скасування сертифіката.

Бібліотека забезпечує:

- Генерацію ключів користувачів із формуванням запитів у форматі PKCS#10.
- Засвідчення запитів на сертифікат із формуванням запитів у форматі PKCS#7.
- Засвідчення запитів на сертифікат із формуванням стартових сертифікатів.
- Збереження сформованих запитів та стартових сертифікатів у БД ЦР.
- Формування заявок на блокування, відновлення та скасування сертифікатів.
- Контроль статусу сформованих запитів на сертифікат та заявок на блокування, відновлення та скасування сертифікатів.
- Контроль статусів сертифікатів на основі CBC (та дельта-CBC), який зберігається у БД ЦР.
- Пошук та отримання X.509-об'єктів із контейнерів особистих ключів.
- Збереження та видалення сертифікатів на НКІ.
- Отримання текстового представлення X.509-об'єктів у форматі HTML.

- Пошук дескрипторів X.509-об'єктів у БД ЦР.
- Видалення X.509-об'єктів, сформованих поточним адміністратором та оператором реєстрації їх БД ЦР.
- Управління контейнерами особистих ключів адміністраторів та користувачів:
 - Зміна ключів з формування запиту на сертифікат.
 - Збереження запиту на сертифікат у БД ЦР.
 - Реєстрація сформованого сертифіката та введення у дію ключів.

Загальні технічні характеристики

Засоби підсистеми управління ключами та сертифікатами СКЗІ «Шифр-Х.509» мають можливість працювати у цілодобовому режимі. Інтерфейси обслуговуючого персоналу та користувачів засобами підсистеми управління ключами та сертифікатами, відповідають вимогам Windows Interface Guidelines For Software Design.

Продуктивність СКЗІ «Шифр-Х.509»:

- Кількість користувачів, які потенційно можуть обслуговуватися засобами ЦСК – не менше 10 000 000 осіб.
- Кількість користувачів, які потенційно можуть обслуговуватися засобами ЦР – не менше 10 000 000 осіб.
- Час формування сертифіката в ЦСК (за наявності запиту на сертифікат та іншої необхідної інформації) – не більше 1 хвилини.
- Час реєстрації користувача в ЦР (за наявності необхідної інформації) – не більше 1 хвилини.
- Час автоматизованого формування запитів у ЦР (за наявності необхідної інформації) – не більше 1 хвилини.
- Час перевірки цілісності та достовірності сертифіката відкритого ключа користувача – не більше 1 секунди.
- Час перевірки цілісності та достовірності електронної позначки часу – не більше 1 секунди.

У засобах СКЗІ «Шифр-Х.509» та її складових елементів реалізовані наступні види діагностики:

- Автоматична перевірка цілісності елементів системи при кожному старті;
- Автоматична перевірка правильності виконання криптоперетворень (при ініціалізації роботи бібліотек криптографічних функцій).

Вказані перевірки проводяться із застосуванням вбудованих засобів контролю.

Характеристики надійності:

- Для засобів ЦСК (ЦР) час на відновлення працездатності після збоїв та аварій, за умови наявності працездатного апаратного забезпечення зі встановленою резервною копією системного ПЗ та ПЗ ЦСК (ЦР), не перевищує 20 хвилин.
- Для МГК час на відновлення працездатності після аварій та збоїв, за умови наявності працездатного апаратного забезпечення зі встановленим системним ПЗ та наявністю справного НКІ, не перевищує 10 хвилин.
- Бібліотеки криптографічних функцій СКЗІ «Шифр-Х.509» не погіршують надійність засобів, у складі яких вони працюють.

Інформація про збереження даних у СКЗІ «Шифр-Х.509» для відновлення працездатності при аваріях:

- Резервному копіюванні підлягають дані, які зберігаються у БД ЦСК, ЦР, TSP-сервера та LDAP-каталозі (для вказаних БД може застосовуватися, як автоматизована, так і ручна система резервного копіювання) та журнали аудиту.
- Резервне копіювання повинно здійснюватися щодобово.

Інформація про персонал для експлуатації засобів підсистеми управління ключами та сертифікатами СКЗІ «Шифр-Х.509»:

- Мінімальний склад посадових осіб ЦСК – 4 особи:
 - адміністратор реєстрації (освіта не нижче середньої технічної);
 - адміністратор сертифікації (вища освіта);
 - адміністратор безпеки та аудиту (вища освіта);
 - системний адміністратор (вища освіта).
- Мінімальний склад посадових осіб Відокремленого пункту реєстрації – 4 особи:
 - адміністратор реєстрації (освіта не нижче середньої технічної);
 - адміністратор сертифікації (вища освіта);
 - адміністратор безпеки та аудиту (вища освіта);
 - системний адміністратор (вища освіта).

Характеристика видів забезпечення

Системне та спеціальне програмне забезпечення

Засоби СКЗІ «Шифр-Х.509» функціонують під управлінням ОС:

- Клієнтські робочі місця: Microsoft Windows 7/10 (x86 чи x86-64).
- Сервера OCSP, TSP, Сервер застосувань ЦСК: Microsoft Windows 2008/2012/2016/2019 (x86-64).
- Сервера LDAP, БД ЦР: RHEL 8/CentOS 8/ (x86-64).

У якості СУБД, яка забезпечує функціонування ЦСК, ЦР та МГК використовується Firebird версії 2.5+.

У якості засобів, які забезпечують роботу LDAP-сервера, використовуються OpenLDAP 2.4+.

Технічне забезпечення

Мінімальні характеристики апаратних засобів, які забезпечують стійку роботу системи наведені у Керівництві з розгортання [\[1\]](#).

Джерела

1. СКЗІ «Шифр-Х.509». Керівництво з розгортання.
2. СКЗІ «Шифр-Х.509». Методика захисту особистого ключа ЦСК.
3. СКЗІ «Шифр-Х.509». Інструкція з порядку генерації ключових даних.
4. СКЗІ «Шифр-Х.509». Інструкція з забезпечення безпеки експлуатації ЦСК.